C.1 BACKGROUND

The U.S. Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program Office has responsibility for overseeing and assisting Government-wide and Agency-specific efforts to provide risk-based and cost-effective cybersecurity, per the Office of Management and Budget (OMB) Memoranda M-14-03 and M-15-01. The cyber landscape in which Federal agencies operate is constantly changing and dynamic. Threats to the nation's information security continue to evolve, and Government leaders have recognized the need for a modified approach in protecting our cyber infrastructure. One approach, CDM, moves away from historical compliance reporting toward combating threats to the nation's networks on a real-time basis. The CDM Program enables DHS, along with Federal Agencies, state, local, regional, and tribal governments, with the ability to enhance and further automate their existing continuous network monitoring capabilities, correlate and analyze critical security-related information, and enhance risk-based decision making at the Agency and Federal enterprise level. The CDM Program benefits participating Agencies by helping to identify security issues so that Agencies can develop better remediation strategies and priorities.

DHS, operating as the lead agency for the CDM Program on behalf of participating Federal Agencies, has a requirement to provide, leverage, and/or expand upon existing Agency CDM tools and sensors (**NOTE:** the use of “tools and sensors” in the TOR encompasses and can often be used interchangeably with “CDM products”). The CDM tools and sensors enable continuous monitoring and diagnostics in support of mitigation activities designed to strengthen the security posture of the Federal civilian .gov networks. Specifically, the tools and sensors will benefit the CDM Program by providing the following:

a. Simplify the security authorization process by helping to automate security assessments.
b. Continuously monitor and report system security status to Agency information security personnel via the Agency CDM Dashboard. (The Government and its CDM Dashboard Provider, Metrica Team Venture (MTV), are developing the Agency CDM Dashboard via a separate TO.)
c. Provide specific details to help prioritize remediation efforts.
d. Allow system owners, risk managers, authorizing officials, and other stakeholders to make better risk-management decisions.
e. Report the security posture of Agency information technology (IT) assets to the future Federal Dashboard, reducing the requirement for manual inputs.

This Group F TO (TO2F) provides support to the non-Chief Financial Officer (CFO) Act Federal Agencies and their components identified in section C.1.2.

C.1.1 PURPOSE

DHS, operating on behalf of Federal agencies, requires a CMaaS Solution for the Agencies and their components identified in this TO. The CMaaS Solution shall provide CDM tools and sensors that implement a common set of capabilities.

C.1.2 AGENCY MISSION

The DHS mission is to safeguard and secure cyberspace in an environment where the cyber attack threat is continuously growing and evolving. The CDM Program defends Federal IT networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, and CMaaS to strengthen the security posture of Government networks.

The CDM Program is managed within the DHS National Protection and Programs Directorate, (NPPD)/Office of Cybersecurity and Communications (CS&C)/Network Security Division (NSD). DHS has been given the authority and funding to implement the CDM program. By centrally managing and funding this program, the DHS CDM Program Office will ensure that the approach to continuous monitoring is consistent, meets a common set of capabilities, and leverages centralized acquisition to improve the speed of procurement. It will achieve significant discounts by consolidating like Federal requirements into "buying groups."

The CDM Program Management Office (PMO) and Technical Point of Contact (TPOC) for this TO are part of the NSD/CDM PMO Branch. The specific Agencies that are supported by this TO are listed in the table below:

Reference #	Full Agency Name	Agency Abbreviation
1	American Battle Monuments Commission	ABMC
2	Broadcasting Board of Governors	BBG
3	Consumer Financial Protection Bureau	CFPB
4	Commodity Futures Trading Commission	CFTC
5	Council of the Inspectors General on Integrity and Efficiency	CIGIE
6	Corporation for National and Community Service	CNCS
7	Consumer Product Safety Commission	CPSC
8	Court Services and Offender Supervision Agency for DC	CSOSA
9	Defense Nuclear Facilities Safety Board	DNFSB
10	Department of State Office of the Inspector General	DOS OIG
11	Equal Employment Opportunity Commission	EEOC
12	Farm Credit Administration	FCA
13	Federal Elections Commission	FEC
14	Federal Energy Regulatory Commission	FERC
15	Federal Housing Finance Agency	FHFA
16	Federal Maritime Commission	FMC
17	Federal Trade Commission	FTC
18	International Boundary and Water Commission	IBWC
19	Millennium Challenge Corporation	MCC

Reference #	Full Agency Name	Agency Abbreviation
20	Merit Systems Protection Board	MSPB
21	National Archives and Records Administration	NARA
22	National Capital Planning Commission	NCPC
23	National Endowment for the Arts	NEA
24	National Endowment for the Humanities	NEH
25	National Labor Relations Board	NLRB
26	National Transportation Safety Board	NTSB
27	Office of Government Ethics	OGE
28	Overseas Private Investment Corporation	OPIC
29	United States Office of Special Counsel	OSC
30	Occupational Safety and Health Review Commission	OSHRC
31	Pension Benefit Guaranty Corporation	PBGC
32	Privacy and Civil Liberties Oversight Board	PCLOB
33	Peace Corps	Peace Corps
34	Postal Regulatory Commission	PRC
35	Railroad Retirement Board	RRB
36	U.S. Securities and Exchange Commission	SEC
37	Selective Service System	SSS
38	Tennessee Valley Authority	TVA
39	United States Access Board	USAB
40	U.S. African Development Foundation	USADF
41	United States International Trade Commission	USITC
42	USPS Office of Inspector General	USPS OIG
43	Federal Communications Commission	FCC
44	Export Import Bank of the United States	EXIM

NOTE: The use of the term “Agency” throughout the TOR refers to the distinct Agencies listed here and their components. It also refers to the end users of the CMaaS Solutions the contractor provides under this TO. The term “DHS” generally refers to the Department hosting the CDM Program Office.

C.2 SCOPE

The contractor shall design, build, and operate a CMaaS Solution for the Agencies identified in this TO. The CMaaS Solution shall include tools, sensors, CMaaS integration support services, and the use of secure Shared Services as the platform for tools, sensors, and supporting CDM infrastructure. The CMaaS integration support services include the planning, provisioning, configuration, operation, and management of tools, sensors, dashboards, and data feeds as well as support for CDM governance. This TO’s scope also includes implementation and maintenance of the CDM Dashboard at the Agency level. The contractor shall provide Agency-specific training for the CMaaS Solution, the Agency CDM Dashboard, and CDM governance.

Some of the aforementioned Agencies currently possess significant IT infrastructure in support of CDM and only require additional base capabilities and services to complement their existing investment in order to achieve the goals of CDM, while others require a full CMaaS Solution. This TO is for CDM tools and sensors and the associated CMaaS integration support services in support of the participating Agencies identified above, to fill gaps in the Agencies' existing continuous monitoring services by installing tools and sensors to reach a common set of capabilities (refer to Table 1 in section C.2.2 Scope – Product Functional Area Scope).

The contractor shall purchase CDM tools and sensors using multi-tenant (cloud) perpetual licenses to the maximum extent possible. This applies to tools and sensors that reside on the shared services platform (SSP). Tools and sensors resident on endpoints, Agency servers, and other similar devices shall also be perpetual to the extent possible.

The Government will assess the CMaaS Solution in accordance with the DHS Security Authorization Process Guide. The CDM PMO will contract for (and pay for) a third party vendor authorized to perform independent validation of the security controls after the controls are ready (see C.6.11.3 and **Section J, Attachment Y**).

In the various technical and management environments of the aforementioned Agencies, the contractor shall ensure that all enumerated tasks are completed. In this TO, the contractor's role may be one of the two following scenarios:

- Full support scenario - develop the solution, transition the solution to operations, then maintain and operate the solution.
- Gap-fill scenario – purchase and transfer CDM tool licenses to approved Agencies to bring their onsite CDM tools to full capacity.

In either scenario, the tools will feed the CDM Agency dashboard, hosted on the Shared Service solution.

C.2.1 SCOPE - IT GOVERNANCE MODELS

The CDM Shared Services Solution proposed must recognize and incorporate the IT governance models in place at participating Agencies. Small Agencies may or may not have a centralized acquisition model. In the centralized model, top-down responsibility for IT acquisition, solutions delivery, conceptualizing, developing, and implementing IT solutions for all parts of the business is controlled by the Agency in one place. This is usually a headquarters (HQ) function, but may also be delegated to one of the Agency's larger components. Small Agencies may also leverage shared acquisition offices for cost savings purposes or utilize a centralized-like model without having the benefit of an official acquisitions office.

C.2.2 SCOPE – PRODUCT FUNCTIONAL AREAS

The Product Functional Area scope of this TO is limited to CDM Phase 1 and Phase 2 only, as noted in Table 1: CDM Capabilities Scope (i.e., Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Setting Management (CM), Vulnerability Management (VUL), Manage Trust in People granted Access (TRUST), Manage Security Related Behavior (BEHAVE), Manage Credentials and Authentication (CRED), and Manage Account Access (PRIV)).

Network Access Controls (NAC), Mobile, and cloud assets are not in scope of this TO. Future CDM Tool functional areas will be covered by future TOs. Disaster recovery capability is required for the Shared Services assessment and authorization (A&A) boundary but not for items outside the A&A boundary.

Table 1 – Product Functional Area Scope

Functional Area	In Scope	Out of Scope
CDM Phase 1		
HWAM	End point (Workstations, Servers); Network Devices (infrastructure)	Mobile Devices (8); Cloud-Based Assets (7)
SWAM	Operating System (1), Common Applications (2), Other Applications (3), Application Integrity (e.g., Whitelisting) (4)	Mobile Devices (8), Cloud-Based Assets (7), Code Validation (5)
CM	Operating System (1), Common Applications (2)	Mobile Devices (8); Cloud-Based Assets (7), Database (DB)/Web Common Weakness Enumerations
VUL	Operating System (1), Common Applications (2)	Mobile Devices(8); Cloud-Based Assets (7); DB/Web Common Weakness Enumerations (CWEs) (6)
CDM Phase 2		
TRUST	Agency Users/Accounts (9) within scope of Phase1	Accounts for Cloud/Mobile Assets
BEHAVE	Agency Users/Accounts (9) within scope of Phase1	Accounts for Cloud/Mobile Assets
CRED	Agency Users/Accounts (9) within scope of Phase1 coverage	Accounts for Cloud/Mobile Assets
PRIV	Agency Users/Accounts (9) within scope of Phase1 coverage	Accounts for Cloud/Mobile Assets

1. *Operating System* - As defined in the National Vulnerability Database (NVD) product category of "Operating System" within the Common Platform Enumerations (CPEs).

2. *Common Applications* - Generally defined in NVD as not "Operating System," to include categories as "desktop application" or "database management" for the CPE.

3. *Other Applications* - Software that does not have identification within NVD (SWAM).

4. *Application Integrity* - The part of SWAM that assures the asset identified is a correct and proper instance and is fully authorized. This is usually done through a whitelisting tool and method (SWAM).

5. *Code Validatio*n - The part of SWAM that assures the code used to create applications does not contain vulnerabilities.

6. *DB/Web CWEs* - This is for products specifically designed to manage Database/Web vulnerabilities or configuration settings and reporting in the form of CWEs versus Common Vulnerability Enumerations (CVEs).

7. *Cloud Assets* - As defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The nature of the dynamics for shared resources provides challenges to the timing windows within traditional asset tracking.

8. *Mobile Devices* - As defined in NIST SP 800-124 Rev 1, "The following hardware and software characteristics collectively define the baseline of mobile devices:

   a. A small form factor.
   b. At least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the Internet or other data networks.
   c. Local built-in (non-removable) data storage.
   d. An operating system that is not a full-fledged desktop or laptop operating system.
   e. Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties)."

9. *User* - A generic term that applies to any entity (including non-person entities) that access any resource, physical or logical, in an organization.

10. *Account* - The means by which a user can access a system.

C.2.3 SCOPE – CDM SOLUTION

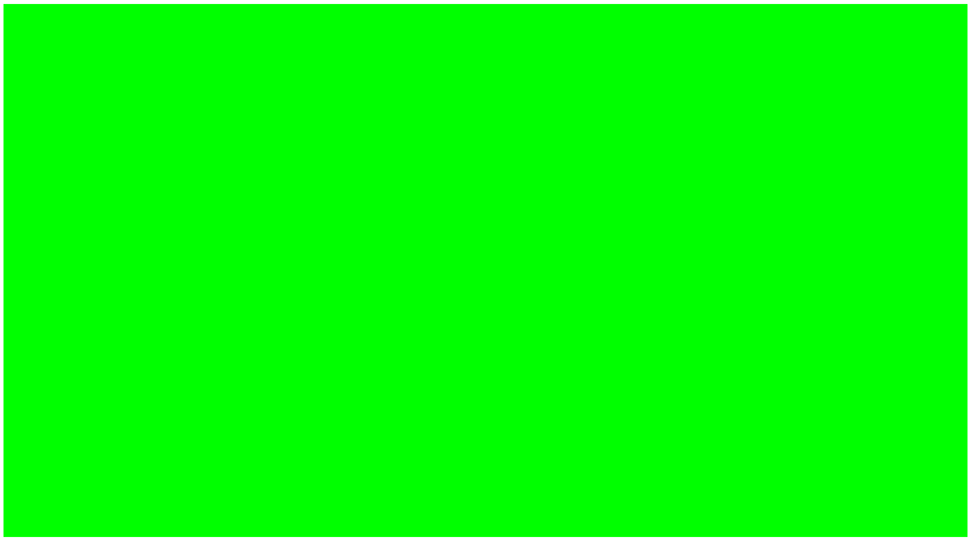
For this TO, the CDM solution is divided into two primary structures. The first is the "shared service" (C.2.3.1); while the second is the support for the CDM functional areas (C.2.3.3). This section describes those two structures, plus design constraints for communications between the shared services and the Agencies (C.2.3.2) and constraints for shared services to make them private (C.2.3.4).

C.2.3.1 SCOPE – SHARED SERVICES

Note, this section states requirements and describes key concepts for the design of CDM Shared Services that the contractor shall fulfill; however, these descriptions are also applicable to offerors for use in the preparation of the Technical Solution in their technical proposal.

a. **CDM Shared Service Objective:** CDM Shared Service extends the current capabilities of the existing DHS CDM program into a delivery model that adheres to the core principles of a shared service. The contractor shall procure CDM tools from the CDM CMaaS Blanket Purchase Agreement (BPA) (H.8.1) (and appearing in the Catalog of Tools Available on Any CDM CMaaS BPA (**Section J, Attachment V)**).

Figure 1: Shared First Strategy's IT Shared Services Concept Overview



The CDM Shared Service directly supports the *Federal Cloud Computing Strategy* ("Cloud First")[1] and the *Federal Information Technology Shared Services Strategy* ("Shared First")[2]; while meeting the security objectives of CDM. The CDM Shared Service is expected to yield significant benefits for Agencies. Agencies will realize cost savings, reduced impacts to

[1] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf
[2] https://www.dhs.gov/sites/default/files/publications/digital-strategy/shared-services-strategy.pdf

infrastructure, and reliable service levels, as well as the maintenance and improvement of their security postures.

Figure 1 represents DHS's vision for supporting both the "Cloud First" and "Shared First" (highlighted in red (gray in non-color reproduction)) strategies of the Federal Government tailored to support the CDM Program.

This figure is derived from page 5 of Executive Office of the President report, "Federal Information Technology Shared Service Strategy," dated May 2, 2012. The red highlights show how the SSP to be provided under this TO shall conform to the shared services model called out in the cited Shared Services Strategy document.

b. **Special Considerations for CDM Shared Service Design:** The contractor shall design the CDM Shared Service architecture under a new model for delivering CDM that reflects the following principles:

i. **Cloud principles:** CDM Shared Services shall deploy to a scalable, elastic hosting environment in order to minimize infrastructure costs.

ii. **Shared services principles:** CDM Shared Services shall serve many customers and be available through standard interfaces (e.g., web browsers).

iii. **Service Level Objectives (SLOs):** CDM Shared Service's design shall support the Service Level Objectives specified in the contractor's Quality Control Plan (QCP) (**Section F, Deliverable 4**) and outlined in the QASP (**Section J, Attachment C)**.

iv. **Risk distribution:** The CDM Shared Service shall store elements of secure Agency data; therefore, the contractor shall protect those elements within the CDM Shared Service operating environment.

v. **Adherence to Federal security policy:** The CDM Shared Service shall be accredited and operated in accordance with all applicable Federal security policies, including the Federal Information Security Management Act (FISMA), OMB, NIST, and DHS guidelines.

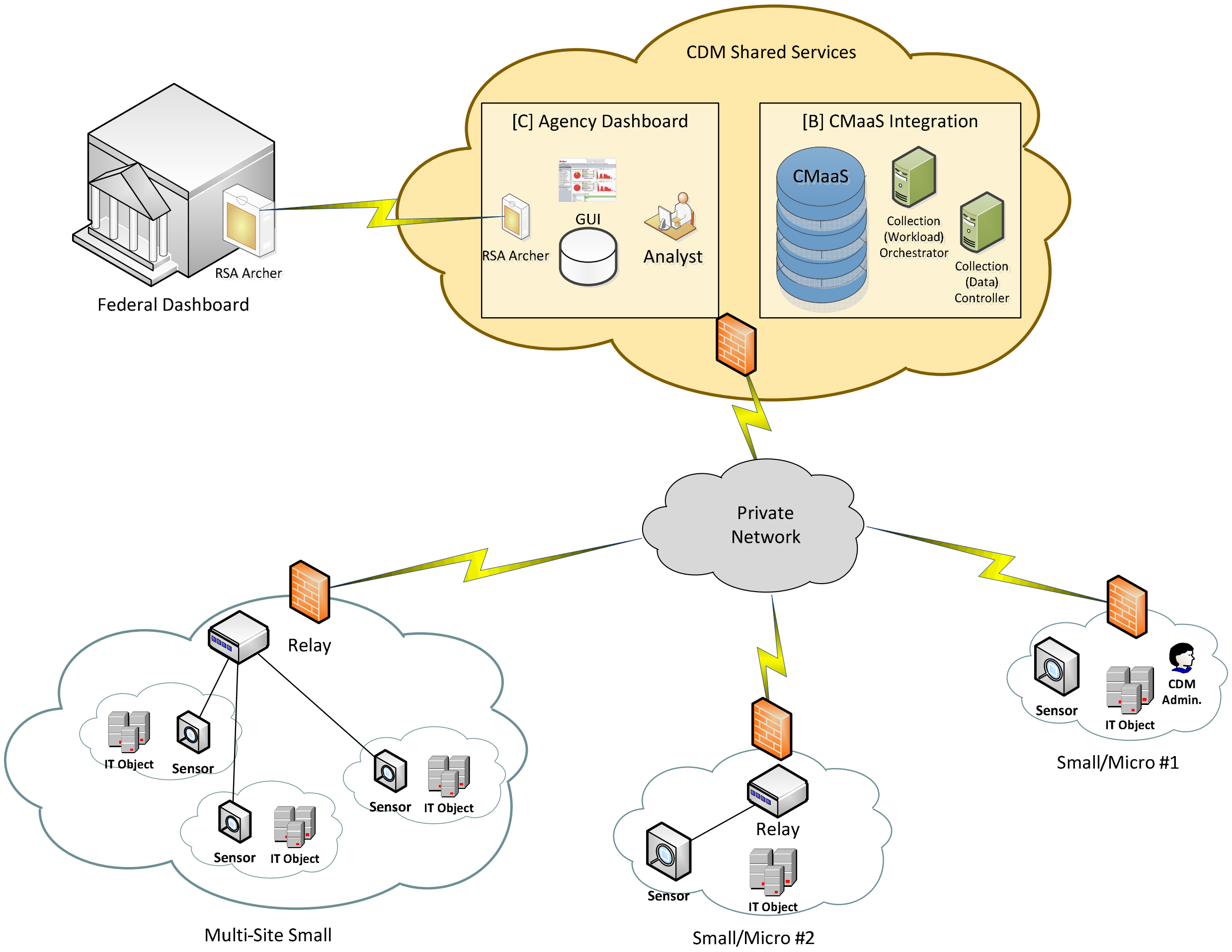
vi. **Licensing:** All perpetual licenses for CDM tools and sensors shall be held by DHS and must support a multi-tenancy requirement. There may be select cases where licenses will be transferred to participating agencies.

vii. **Infrastructure:** DHS will not procure or own the Shared Service infrastructure (hosting environment). The shared services infrastructure shall not be co-mingled with non-Government data and shall be located entirely within the continental United States (CONUS). ("Government" includes United States federal, state, local, and tribal Governments for the purposes of this requirement.)

The CDM Shared Service solution proposed shall be compliant with the CDM High Impact Security Controls **(Section J, Attachment Y).**

Figure 2 is a conceptual diagram of the shared service for CDM, including the use of network connections from the SSP to the Agencies participating in this solicitation (e.g., Small/Micro #1). The shared service architecture shall not allow access to the Internet. The shared services shall comply with Trusted Internet Connection (TIC) Security Pattern #3[3] for Government to Government Intra-Agency Connections.

Figure 2: CDM Shared Services Conceptual Architecture



The Shared Services Conceptual Architecture in Figure 2, Administrative Channel Management Node in Figure 3, and the Operational Views in Figures 4 through 7 can be interpreted as follows:

[3] Security Pattern #3 In Accordance With (IAW) TIC Reference Architecture Document Version 2.0 dated October 1, 2013.

a. Sensors - Software and/or hardware tools from the CDM CMaaS BPA that capture cybersecurity information about an Agency's hardware, software, and network, such as information about a hardware asset used for HWAM. Sensors may also use installed technology (e.g., an endpoint's operating system). Note, depiction of Sensors in the Agency's site in these Figures is not meant to imply that CDM CMaaS BPA cybersecurity tools must be located at these sites.

b. Relays or Relay/Aggregator - Software and/or hardware tools from the CDM CMaaS BPA or general purpose IT that may process (e.g., concentrate or reformat) and forward cybersecurity data captured by a sensor to a consumer of that data, such as a Dashboard or the SSP.

c. Firewall - "A gateway that limits access between networks in accordance with local security policy." Source: SP 800-32/ "A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy." Source: CNSSI-4009 / "A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures." Source: SP 800-41

d. CDM Shared Services Infrastructure – Software and/or hardware tools residing on the SSP platform that receive, process, and forward cybersecurity information.

e. CDM Shared Services Data – Cybersecurity data captured by sensors, possibly processed (e.g., concentrated, summarized, or reformatted) and stored for further use. For TO2F, stored on the SSP.

f. Encrypted Link - Communications security that encrypts and decrypts all traffic at each end of a communications link. Source: Wikipedia

g. Cert-Based Encryption - A system in which a certificate authority uses ID-based cryptography to produce a certificate. This system gives the users both implicit and explicit certification. Source: Wikipedia

h. A&A Boundary – The boundary of an IT system within which assessment and authorization occurs.

i. Arrows - Indicate the direction(s) in which data communications pass.

j. D/A – Agency

k. SSP – Shared Services Platform

l. CSP – Cloud Service Provider (the same as SSP)

C.2.3.2 SCOPE - SHARED SERVICES COMMUNICATIONS OPERATIONS

This section describes possible alternative high level designs (operational views) of communications links and operations between the SSP and Agency IT. The contractor shall structure the Shared Services' communications with the target Agencies (C.1.2) using connections that conform to one (or more, for multiple connections) of the operational concepts depicted in Figures 4 through 7.

These Figures show only key elements of the SSP/Agency connectivity. The contractor shall provide the underlying hardware, software, and network infrastructure that supports one of the depicted operational views (or more, for multiple connections) but that excludes any elements that would violate the secure communications protocols and constraints that the operational views depict.

The Technical Solution shall provide secure network connections from the CDM Shared Services environment to each Agency included in this TO, ensuring Trusted Internet Connection (TIC) compliance utilizing Security Pattern #3 (Intra-Agency or Government to Government connection). These connections shall not traverse the Internet except via a secured point-to-point circuit or tunnel.

C.2.3.2.1 BOUNDARY PROTECTION

Boundary protection for these connections includes the following:

a. Packet Filtering (Required)
b. EINSTEIN Intrusion Detection system. NOTE: This device cannot be installed or located outside the United States. (Required)
c. Content Filtering (Desirable)
d. Authentication (Desirable, except where noted)
e. Methodology for creating separate communication channels for user, data and administrative functions, as follows:

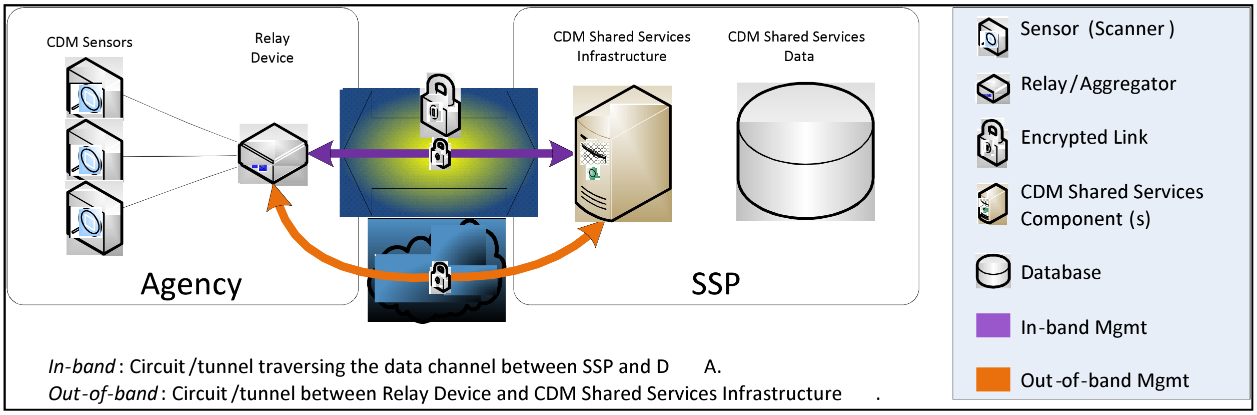
i. User Channel: network communication paths and/or links that pass data between the Agencies' users and the SSP portals. Uses include monitoring and analysis of CDM collections, accessing the CDM posture assessment report on the CDM Agencies' dashboard(s) and reviewing shared service management.

ii. Data Channel: These communication paths and/or circuits shall connect sensors and relays with the CDM Collector at the SSP. These channels shall be encrypted due to the sensitive nature of the information contained within this channel (e.g., vulnerability data).

iii. Administrative Channel: The Administrative Channel carries all communications (e.g. policy updates, configuration changes) between the Agencies and the CDM Shared Services elements at the SSP as shown in Figure 2. These types of communication channels shall use FIPS 140-2 encryption and two-factor authentication. Figure 2 shows the high level connectivity path for both in-band and out-of-band management. The type of management path used is dependent upon the Operational View used. Operational Views are depicted in Figures 4 through 7.

Figure 3 depicts Administrative Channel Management, which is described in the immediately preceding bullet.

Figure 3: Administrative Channel Management Nodes


CDM Sensors
Relay Device
CDM Shared Services Infrastructure
CDM Shared Services Data
Agency
SSP
Sensor (Scanner)
Relay/Aggregator
Encrypted Link
CDM Shared Services Component (s)
Database
In-band Mgmt
Out-of-band Mgmt
In-band: Circuit/tunnel traversing the data channel between SSP and D A.
Out-of-band: Circuit/tunnel between Relay Device and CDM Shared Services Infrastructure .

C.2.3.2.2 DATA CHANNEL OPERATIONAL VIEWS

Figures 4 through 7 show the Government's scenarios for the data channel architectures that the contractor shall use for CDM Shared Services. The contractor shall design and implement the CMaaS Solution such that the Solution includes connectivity and data channels that can conform to all of the operational views shown in Figures 4 through 7. (Multiple views are needed to address the diverse needs of multiple Agencies and their multiple IT devices, infrastructure, and locations.) CMaaS Solution designs that do not use these operational views are not acceptable unless the contractor's technical solution has convincingly justified that one or more of the operational views are not necessary to support the Agencies.

While these views depict the high level components and data flows that are necessary to support secure communications, these high level designs are not by themselves sufficient to ensure that security and shall be implemented with an appropriately secure low level design and implementation. The contractor shall provide a complete concept of operations (C.6.2.2) and architecture (C.6.2.3) for the CMaaS Solution that incorporates one or more of these views and the additional detail necessary to ensure secure communications, along with the other technical requirements called out in C.2.3.1 and the other sections of this TO.

The Operational Views are conceptual and at a high level of technical detail, but describe both required and prohibited technical functional components (hardware, software, network elements).

a. Required. The depiction of a functional component (e.g., sensors, relays, links) in an operational view means that the contractor's Technical Solution shall provide the functionality of that component, regardless of how the functional component is implemented (e.g., using software, hardware).

b. Prohibited. The depiction of a functional component in an operational view means that the contractor's Technical Solution shall not circumvent or obstruct the functionality of the depicted component, (e.g., shall not provide a path around a firewall or around an encrypted link) that allows communications traffic to flow through the system without the protections that the firewall and encrypted link provide.

Following are figures and descriptions for each view. The contractor shall provide a solution that can meet each Operational View in order to accommodate the varied IT Environments of the Agencies in-scope.

Figure 4: Operational View 1

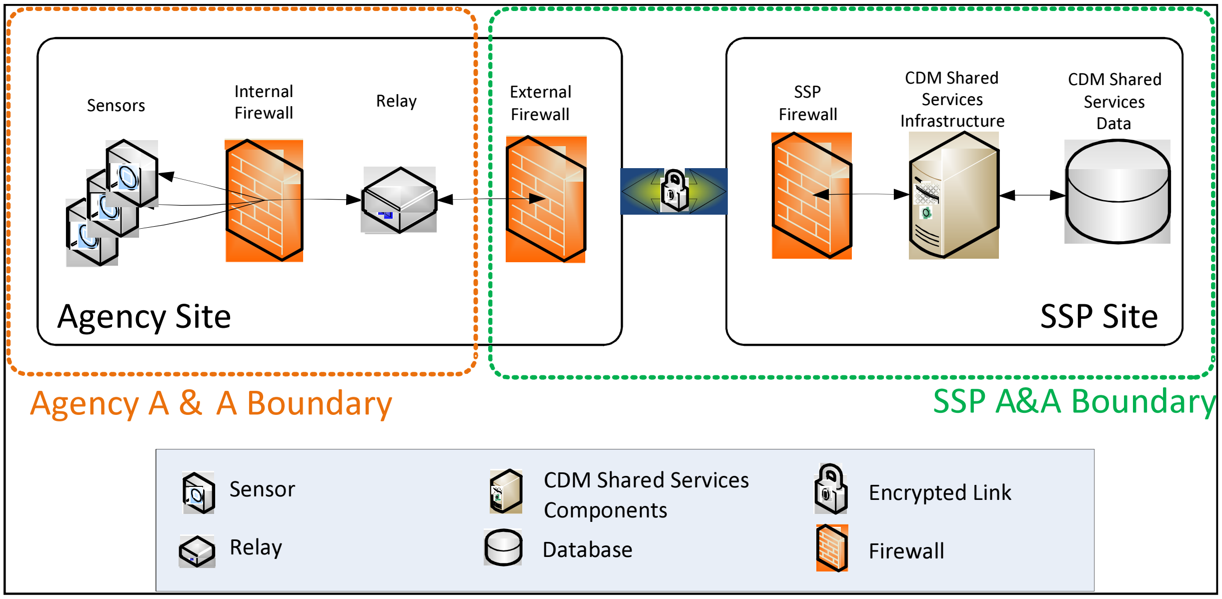


Figure 4 - Operational View 1 (OV$_1$) – Both the Relay and the SSP can initiate a push for CDM data collection. The SSP is connected to an On-Site Relay with Bi-Directional Communications. This OV is the only OV that will support the use of In-band management for the administrative channel (e.g., policy updates, configuration changes). The communication path is secured using an approach that satisfies FIPS 140-2.

Figure 5: Operational View 2

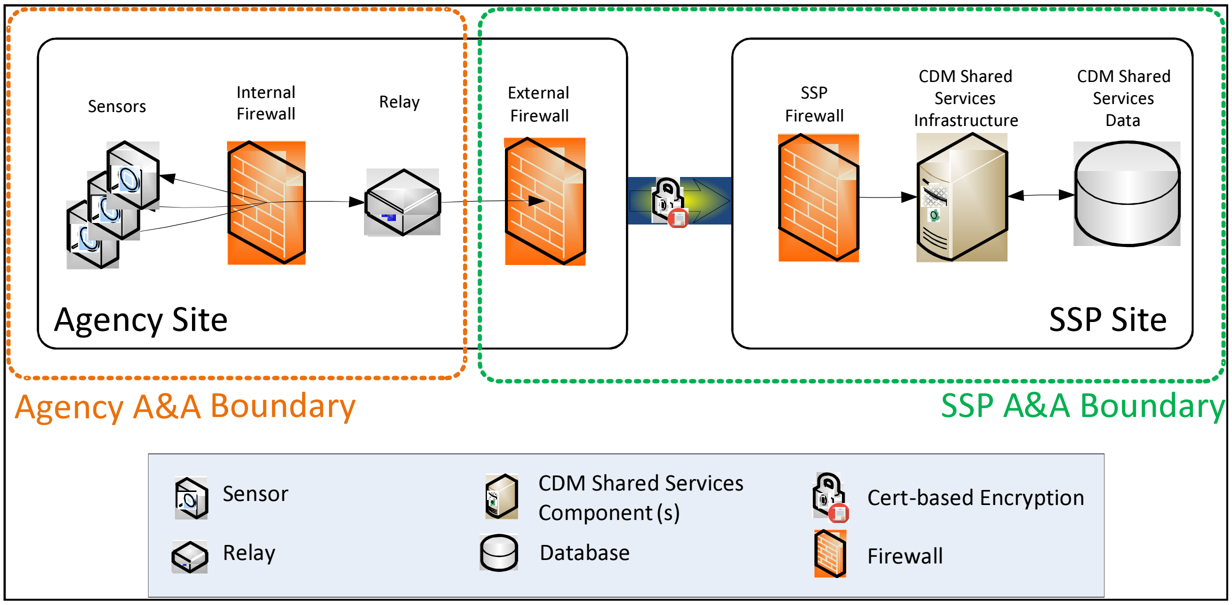


Figure 5 - OV_2 – This OV shows that the SSP must be able to accept a push without creating a connection to the relay. Bi-directional communication only occurs between the sensor infrastructure and the Relay. The communication path between the SSP and the Agencies shall be secured through the use of Private Key Infrastructure (PKI), Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or a comparable method. Out-of Band Management must be used for administrative communication.

Figure 6: Operational View 3

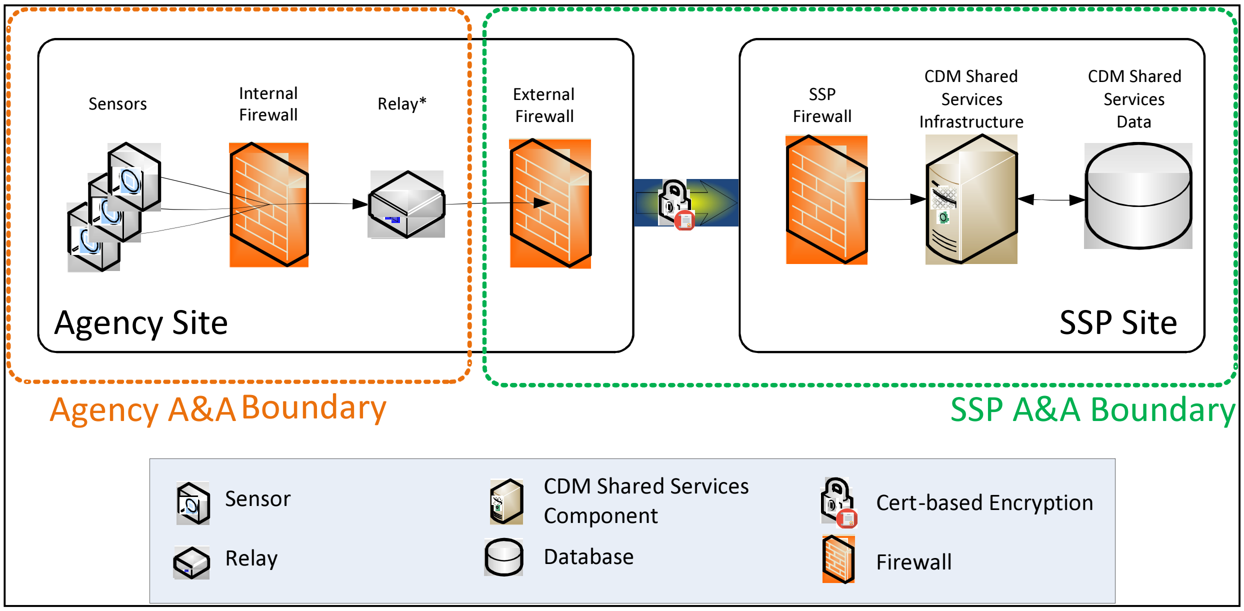


Figure 6 - OV_3 – This OV shows that only the sensors are allowed to initiate a push. Like $OV_{2,}$ the SSP must be able to accept a push. Use of a relay in this OV is optional for the use of sensor suites that support data aggregation. The communication path between the SSP and the Agencies shall be secured through the use of PKI, SSL/TLS or a comparable method. Out-of Band Management must be used for administrative communication.

Figure 7: Operational View 4

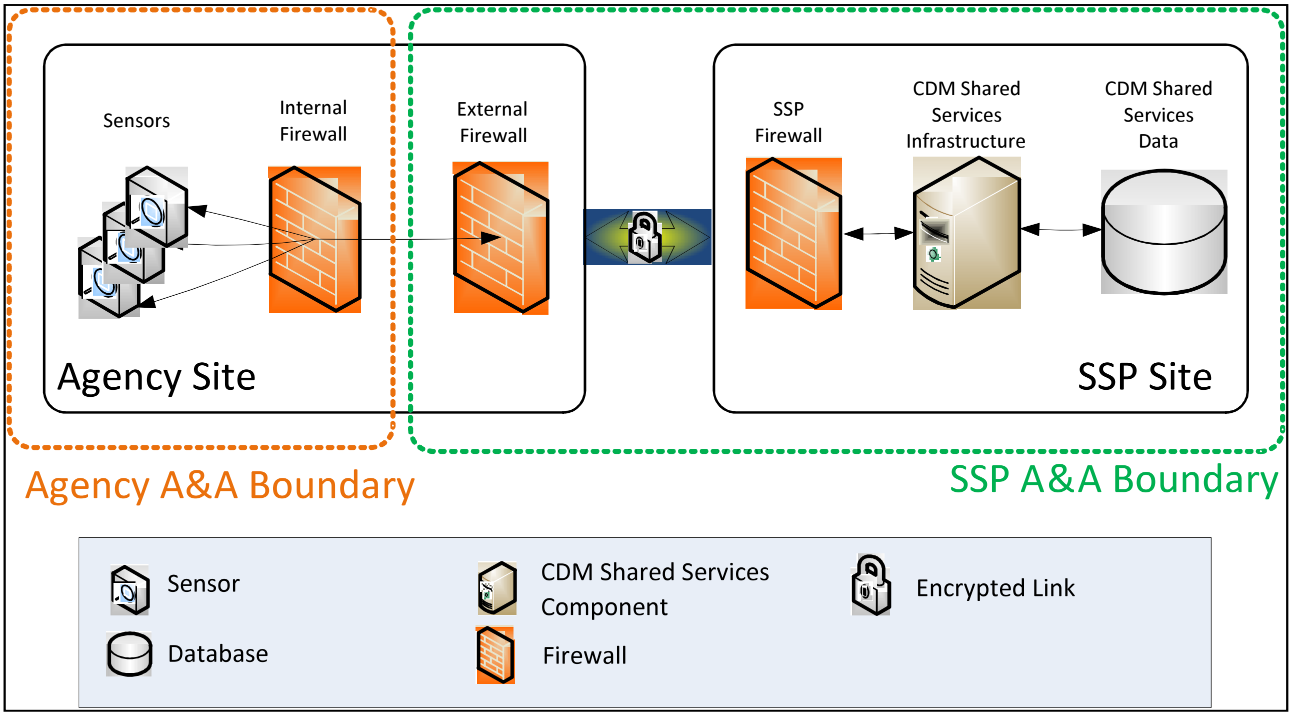


Figure 7 - OV$_4$ – This scenario addresses those participating Agencies who may not have the infrastructure to support equipment installation on-premise or a small/remote site with a minimal number of sensors. Bi-directional communication from sensors (on-demand) without the use of a relay is allowed and the use of relay is not required. The Sensors or the SSP may initiate the push and sensors may be set to transmit data at specific intervals or triggered by the CDM Agency's dashboard via the SSP. The communication path is secured using an approach that satisfies FIPS 140-2.

Aside from these requirements and prohibitions, the contractor’s Technical Solution may provide additional functional components not explicitly shown in the figures that accomplish other requirements of the TO. Additional requirements and desirable features of the depicted Operational Views are described in Figures 4 through 7.

Table 2 summarizes the characteristics of the administrative channel and the four data channel scenario operational views described above.

Table 2: Characteristics of Operational View Data Channel Scenarios

<table>
<tr><th rowspan="2">Characteristic</th><th rowspan="2">Administrative Channel</th><th colspan="4">Operational View Data Channel Scenarios</th></tr>
<tr><th>1</th><th>2</th><th>3</th><th>4</th></tr>
<tr><td><b>Who can initiate a push?</b></td><td rowspan="4">N/A</td><td>Relay/SSP</td><td>Relay</td><td>Sensors</td><td>Sensors/SSP</td></tr>
<tr><td><b>Sensor-relay communication</b></td><td colspan="2">Bi-directional</td><td>Uni-directional</td><td rowspan="2">N/A
(No relay)</td></tr>
<tr><td><b>Relay-SSP communication</b></td><td>Bi-directional</td><td colspan="2">Uni-directional</td></tr>
<tr><td><b>Sensor-SSP communication</b></td><td colspan="3">N/A (Relay in between)</td><td>Bi-directional</td></tr>
<tr><td><b>Agencies-SSP connection</b></td><td colspan="5">Does not traverse Agency’s Internet connection</td></tr>
<tr><td><b>Agencies-SSP path security</b></td><td colspan="2">IPsec VPN, MPLS tunnel, (FIPS 140-2)</td><td colspan="2">PKI certificate, SSL/TLS, or comparable</td><td>IPsec VPN, MPLS tunnel, (FIPS 140-2)</td></tr>
<tr><td><b>Relay present?</b></td><td>N/A</td><td colspan="3">Yes</td><td>No</td></tr>
</table>

C.2.3.3 SCOPE – SUPPORT OF CDM FUNCTIONAL AREAS

Figure 8, below, is adapted from the CDM CMaaS BPA and depicts the overall CDM CMaaS high level architecture, including functional components within the scope of this TO as well as legacy Agency infrastructure, the Federal Dashboard, and other entities that are part of the overall solution. This section explains how the CMaaS Solution to be provided under this TO fits into the overall picture.

The CMaaS Solution shall conform to Figure 8, CDM Functional Areas, which depicts the CDM architecture and four distinct functional/logical areas of the CDM capabilities. The scope of this TO includes Areas “A” and “B.” The scope of this TO also includes integration with the CDM Dashboard TO with the Government-provided Agency CDM Dashboard to meet the requirement in Area “C.” Support for Area “D” (except for connectivity between Agency CDM Dashboards and the Federal Dashboard) is outside the scope of this TO. The Government will flow down policy control from the Federal Dashboard (D) to impact the subordinate Areas of A through C. Figure 8 also depicts the flow of summary-level data for display in the Federal Dashboard. The CMaaS Solution proposed for this TO shall exclude any assets residing in commercial cloud service provider offerings or mobile devices.

Figure 8: CDM Functional Areas

a. Area A is the location for tools and sensors that, together, provide the coverage of the CDM Tool Functional Areas for Phase 1 (HWAM, SWAM, CM, and VUL) and Phase 2 (TRUST, BEHAVE, CRED, PRIV). It is envisioned that CDM Functional Level A will reside within the Agency's infrastructure while all other functional areas will be located in the shared service environment. **NOTE:** Data in commercial cloud service offerings and mobile devices are out of scope of this TO.
b. Area B is the contractor integration point solution that supports the required integration and operational control points for the CMaaS Solution.
c. Area C is the Agency CDM Dashboard(s). The contractor shall integrate the Agency CDM Dashboard(s) into the CDM Shared Service Solution.
d. Area D is the Federal CDM Dashboard. As such, this area has no TO2F contractor responsibilities and is being provided by a separate CDM Dashboard TO.

C.2.3.4 SCOPE - PRIVATE SHARED SERVICES

The contractor shall provide shared services that are private for each Agency. Data from multiple Agencies under this TO can be co-located on the same physical device or within the same data center, provided that Agency privacy is preserved; the choice of devices or locations depends on the contractor's Technical Approach. However, all CMaaS Solution elements (e.g., hardware, network links) shall be located within CONUS. No non-Government tenants shall use the same physical devices as are used by the CMaaS Solution under this TO.

Figure 9 shows some of the functional components of a private shared service, but without specifying how the agencies are separated. Figure 10 shows an example of *segregated separation* for CDM Shared Services; in contrast, Figure 11 shows an example of isolated separation. *Isolated separation* by itself is not feasible under this TO and will not scale adequately for CDM Shared Services. However, a hybrid approach, in which Agencies with similar risk tolerances are segregated in the same isolated instance, can be used as a scalable alternative. There are methods for creating tenant separation either through segregation or isolation. Note the following:

a. In the Isolated Separation (Figure 11), each agency (e.g., D/A 1 (Agency 1)) has its own copy of CMaaS Integration – the Collection Orchestrator, the Collection Controller, and its own Agency Specific Configuration. In contrast, in the Segregated Separation (Figure 10), these functional components are shared by multiple agencies – there is only one instance of the Collection Orchestrator, the Collection Controller, and there is no Agency Specific Configuration. By sharing the CMaaS Integration functional components, IT resources are saved.
b. In the Isolated Separation (Figure 11), each Agency has its own Repository, while in the Segregated Separation (Figure 10), Agencies have different storage areas on a single data base Repository – again, saving IT resources.

The high overhead of agency-specific CMaaS Integration instances depicted in Figure 11 help explain why isolated separation does not scale well and why this TO is structured for shared services that will scale efficiently.

Figure 9: CDM Shared Services Instantiations

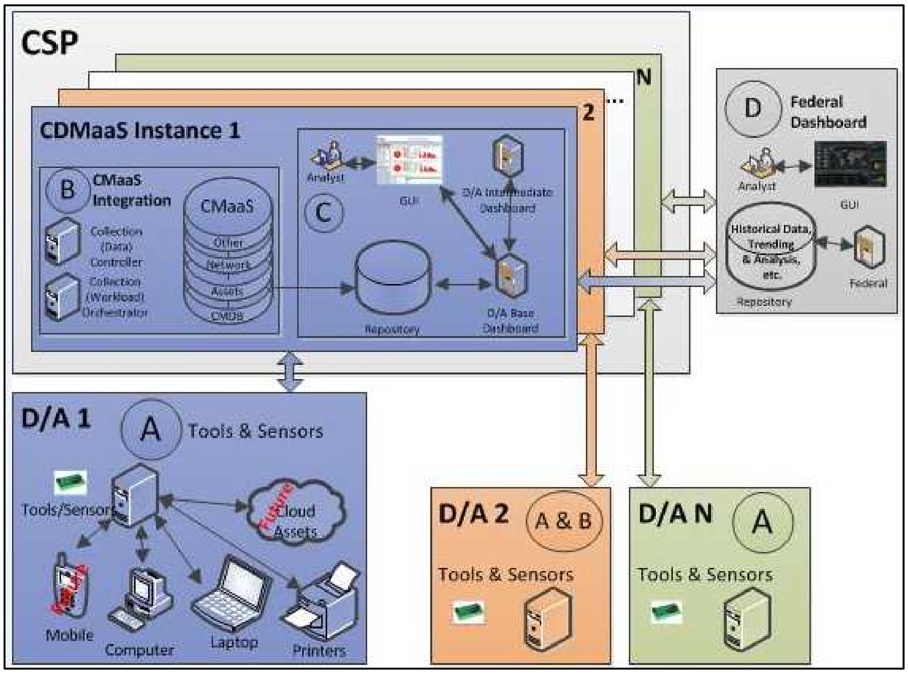
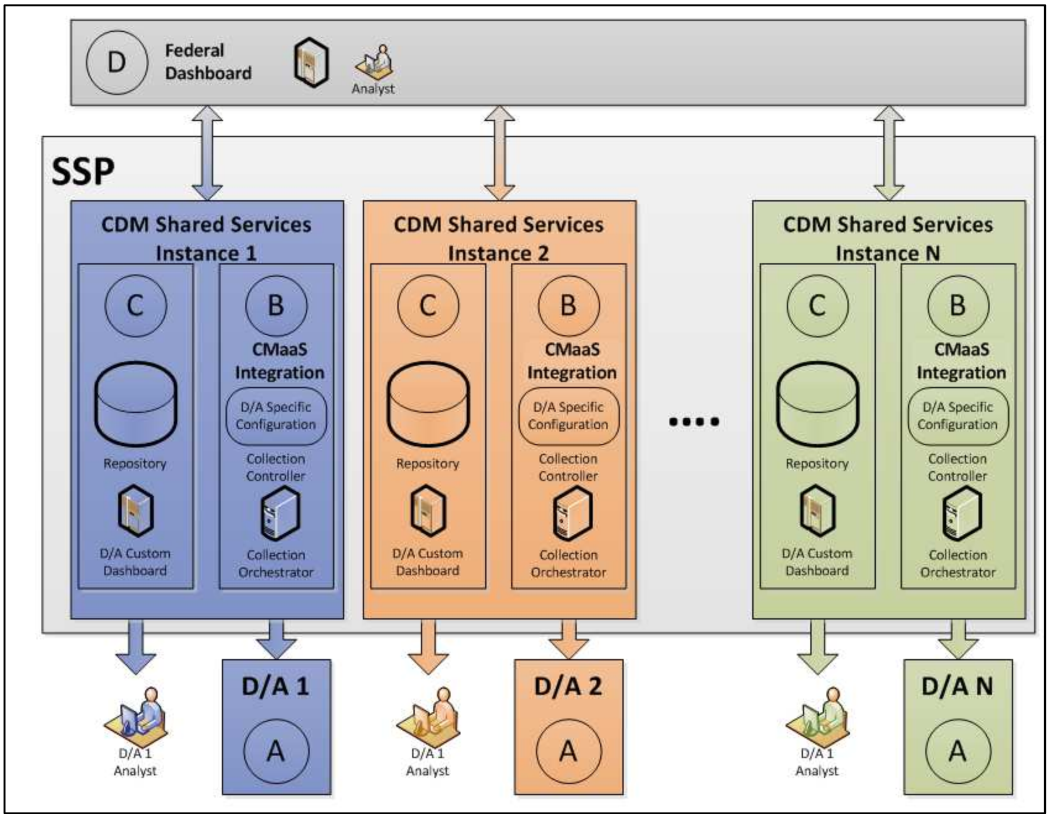


Figure 10: CDM Shared Service Segregation

Figure 11: CDM Shared Services Isolation



NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, comments, with respect to isolation:

> "High degrees of multi-tenancy … are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. To reach the high scales of consumption desired, cloud providers have to ensure dynamic, flexible delivery of service and isolation of consumer resources. Multi-tenancy in IaaS cloud computing environments is typically done by multiplexing the execution of virtual machines from potentially different consumers on the same physical server… Applications deployed on guest virtual machines remain susceptible to attack and compromise, much the same as their non-virtualized counterparts...
>
> ".... Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms…
>
> "A virtual machine monitor can, in theory, be smaller and less complex than an operating system. These characteristics generally make it easier to analyze and improve the quality of security, giving a virtual machine monitor the potential to be better suited for maintaining strong isolation between guest virtual machines than an operating system is for isolating processes..."

(The excerpt above does not imply advocacy for virtualization or any other specific technology for this TO.)

The contractor shall design and implement the shared services such that each Agency can only access its own data and its own Agency Dashboard, and such that only summary level data from the Agencies are transmitted to the Federal Dashboard. The use of physical separation, (e.g., different physical servers); logical separation, (e.g., through a logically partitioned data base); or logical isolation, (e.g., through multiple virtual machines running on the same physical servers), are allowable under this contract, provided that the contractor ensures that Agencies can only read, write, update or delete their own cybersecurity data.

NOTE: The CDM Dashboard will be an online display of the current security status of U.S. Government IT systems. The contractor shall install and maintain Agency CDM Dashboards in the CDM Shared Service center for the participating Agencies, working with the approved vendor of the Dashboard, Metrica Team Venture (MTV) at the appropriate time. The CDM Dashboard is a customized configuration of commercial-off-the-shelf (COTS) software based on RSA Archer and developed under a separate DHS contract.

C.3 CURRENT IT/NETWORK ENVIRONMENT

High-level IT and network infrastructure descriptions are provided in **Section J, Attachment G - Agency IT/Network Environment Summary Information** for each Agency supported by this TO. The summary level IT/Network environment information includes:

Question #	**Agency Information**
1	General Agency Description (short description).
2	Total # of end users in scope of this Task Order – FTEs and contractors.
3	# of desktops (end user devices) including laptops.
4	# Desktop Operating Systems (OS) broken down by OS: (Total #s - MS Windows; *NIX; Apple, other)
5	# of Servers w/ average Core count (Physical and Virtual #s if available).
6	# of Server Operating Systems (OS) broken down by OS: (Total # - MS Windows; *NIX; other)
7	Location and # of major offices, data centers and any other relevant characteristics of the D/A facilities (Government Owned, Contractor Owned, Commercial etc.) and its ability to support additional sensors and tools.
8	Do you have existing security/operations staff and if so, how many?
9	Identify how many staff will have direct interaction with the CMaaS solution and will require training, to include product specific training.
10	Would O&M services potentially conflict/overlap with existing D/A operations and security contracts? (Yes/No)
11	Briefly describe current CDM capability including any tools or sensors that are currently in production.
12	Provide any Agency information that would be relevant to implementation in the FY16 timeframe i.e. • Schedule Conflict

Question #	Agency Information
	- Significant IT Event/Migration - Regulations Specific to your agency (election)
13	Do you have infrastructure space where, if needed, CDM hardware could be installed? Is rack space, redundant and uninterruptible power supply (UPS) power, cabling, etc. available? Does data storage space exist?
14	Does your agency have a policy regarding connecting to an external service provider? (Yes/No)
15	Is IPv6 enabled at your agency (Yes/No):
16	How many HSPD-12 cards have been issued for your agency/department (FTEs and contractors)?
17	What is the number of user accounts?
18	What is the number of privileged user accounts?
19	Do you have a firewall at your network boundary and do you have ports available?
20	Do you currently use network access controls?
21	Do you have a remote access infrastructure for telecommuting and laptops, etc.?
22	Please describe the technologies that provide your remote access? (Microsoft Terminal Servers, Citrix, VPN appliances, etc.). What are the high level characteristics for remote access? (E.g. VPN connection over the internet, Remote Access Service (RAS), dial-in, other)
23	Does your agency have a list of approved software/applications that are authorized for approved hardware? For example, Adobe Acrobat, MS Office, Oracle Database, MS IIS, etc. NOTE: This question is related to application whitelisting (SWAM)
24	Does your agency have the ability to centrally deploy software to all end points across your organization?
25	Do you have a Configuration Management/Change Control Policy for infrastructure Improvements/upgrades/installations?
26	Approximately how long would it take to approve server/network changes (assuming proper testing and documentation)?

CDM Material and other products (including non-BPA CDM Material) in production at participating Agencies.

Product Manufacturer	Product Manufacturer and Model Description	Manufacturer Part # and Specific Product Description	Current Count (# of licenses)	Known Gap in Coverage	Deployment information (High level) and short description list. CDM Phase 1 or 2 (HWAM,SWAM,VUL,CSM, TRUST, BEHAVE, CRED, PRIV) area covered.

C.4 DHS SYSTEMS ENGINEERING LIFE CYCLE (SELC) PROCESS

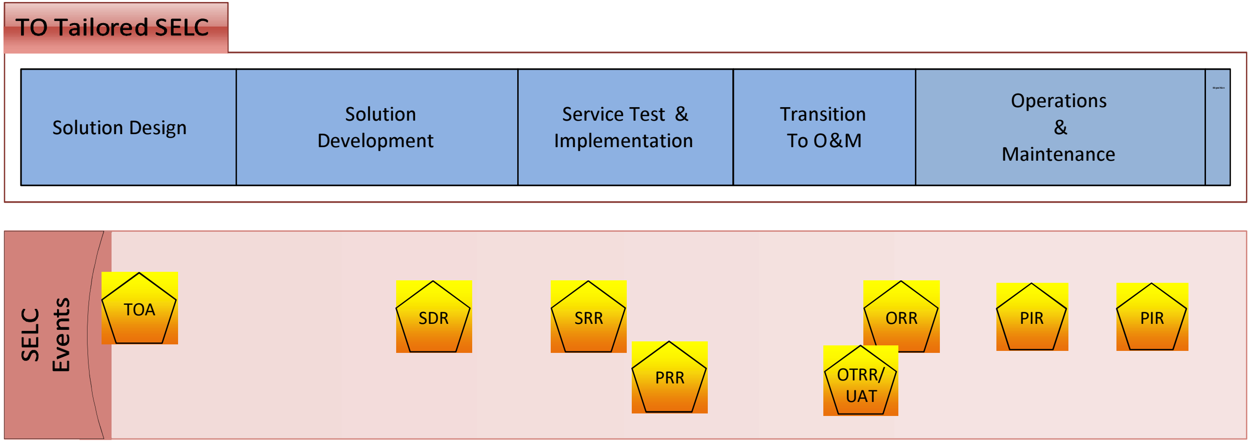
The DHS SELC provides a review process for the design and development of IT solutions, including a structured, formal handoff from developers / designers (engineering) to operations and maintenance staff.

For the purposes of CMaaS, there are four key gates in the SELC, specifically the Solution Design Review (SDR), Service Readiness Review/Production Readiness Review (SRR/PRR), User Acceptance Test (UAT), Operational Readiness Review, and Post Implementation Review (PIR) to include Operational Test Readiness Review (OTRR). For these gates, the contractor shall coordinate with Government stakeholders, including the DHS CDM PMO, GSA FEDSIM, and the participating Agencies, to ensure agreement on solution implementation, schedule, and deliverables necessary approval to proceed to the next phase for each Agency's respective

CMaaS Solution.

The SELC process is governed through reviews that provide the opportunity to assess project progress against a minimal defined set of exit criteria tailored for the program. These reviews provide a knowledge point or mechanism for Government management to determine if and how well a project has completed the necessary activities.

Figure 12: Tailored DHS SELC Process



SELC Event Legend:
SDR - Solution Design Review
SRR- Solution Readiness Review
PRR - Product Readiness Review
ORR - Operational Readiness Review
UAT – User Acceptance Test Review
OTRR - Operational Test Readiness Review
PIR - Post Implementation Review

Factors critical to successful reviews are:

a. All stage activities and exit criteria, as tailored, for each review must be satisfactorily fulfilled, including required documents, in order to proceed; and

b. At each SELC review, the contractor must provide evidence that clearly substantiates the fulfillment of the exit criteria. For example, in testing requirements, test cases designed to validate requirements compliance must successfully produce the required results to be used as evidence of successfully meeting exit criteria. The act of testing in itself is not sufficient evidence if tests fail to produce required results.

The contractor shall follow the DHS SELC process as tailored by the CDM Program to the requirements of this TO as depicted in Figure 12: Tailored DHS SELC Process. The Government's review time is not anticipated to exceed ten business days after receipt by the DHS CDM Program Office of documentation for each SELC review detailed below. The contractor shall coordinate directly with the DHS CDM SELC Team Lead to manage the SELC review process.

C.4.1 SOLUTION DESIGN/DEVELOPMENT PHASE

The contractor shall complete the Solution Design/Development phase at the SDR, where key Government stakeholders will verify that all SDR deliverables are completed and acceptable and that the project baseline scope and schedule are still accurate or need to be adjusted.

The intent of this review is to provide all stakeholders with a common understanding of the solution design that was used as the basis of award [Baseline 0].

The prerequisite documents to enter the SDR are:

1. Overview of CMaaS Solution selection
2. Concept of Operations (CONOPS)
3. System Design to include Data Model/Architecture
4. Proposed deployment
5. Test and Evaluation Master Plan (TEMP)
6. Project Management Plan (PMP)

The specific deliverables are:

1. Documents noted above
2. Presentation materials
3. Baseline schedule (IMS) and Technical Bill of Materials (TBOM)
4. Identification of Next Steps
    a. Plan for resolution of SDR outstanding items
    b. Identification of items needs to SRR
    c. Timeline for SRR

The contractor shall clearly show the Shared Service design within the total solution **(Section F, Deliverable 39)**.

C.4.2 SOLUTION TEST & IMPLEMENTATION PHASE

During this phase, the project transitions from designers to the operations staff. The Government will review the contractor’s CMaaS Solution implemented in an evaluation environment and provide or withhold approval at the SRR. Later, the Government will review the contractor’s CMaaS Solution against requirements of each Agency during the PRR.

The intent of this review is to provide all stakeholders with a common understanding of the design and implementation implications based on revalidation/discovery.

The contractor shall clearly distinguish between Shared Services (**Section F, Deliverable 38**) and CMaaS test and implementation; shall clearly address networking components for small Agencies connecting to Shared Services.

The prerequisite documents to enter the SRR are:

1. Demonstration of CMaaS Solution implementation
2. Initial Security Documentation (e.g., System Security Plan)
3. Initial core solution documentation (e.g., User Manuals)
4. Initial Governance Support Plan

The specific deliverables are:

1. Documents noted above
2. Presentation materials
3. Demonstration of solution
4. Baseline schedule (IMS) and TBOM
5. Identification of Next Steps
   a. Plan for resolution of SRR outstanding items
   b. Identification of items needs to PRR
   c. Timeline for PRR

The intent of PRR is to provide all stakeholders with the specific understanding of the design and implementation implications based on revalidation/discovery for each of the participating Agency environments.

The prerequisites to enter the PRR are:

1. Documentation and requirements for Agencies to move the CMaaS Solution to their environments.
2. Demonstration of integration to the Agency environment (e.g., pilot).

The specific deliverables are:

1. Documents noted above
2. Presentation materials
3. Demonstration of solution (see **Section F**, the Solution includes IT services **Deliverables 40 – COTS CDM Tools, 41 – Data Provided with CDM Tools (if any) and 44 – Ancillary ODCs/Tool**s)
4. Baseline schedule (IMS) and TBOM
5. Identification of Next Steps
   a. Plan for resolution of PRR outstanding items
   b. Identification of items needs to UAT/ORR
   c. Timeline for UAT/ORR

C.4.3 TRANSITION TO OPERATIONS AND MAINTENANCE (O&M) PHASE

The Government will review the contractor's test and evaluation plan execution against the CMaaS Solution based on the requirements of the Agencies and the scope of the TO during the

Operational/User Acceptance RR. The contractor shall complete the Transition to O&M phase at the ORR. Government stakeholders will verify that all deliverables are completed and acceptable, and that operations staff are ready to deploy the CMaaS Solution into production and maintain and support it going forward.

The intent of ORR is to provide all stakeholders with the specific understanding of the ability to transition the solutions to operational status for each of the participating Agency environments.

The UAT documentation shall distinguish between Shared Services and CMaaS. The Responsibility – Accountability – Consulted – Informed (RACI) roles for security controls must be clear for Shared Services.

The requirements to complete the UAT are:

a. Documentation and requirements to move the CMaaS Solution to the operational environments.
b. Documentation of Testing and Results.

The prerequisite to enter the ORR are:

a. Documentation and requirements for Agencies to move the CMaaS Solution to the operational environments.
b. Results of Operational Testing, Security Risk Assessment
c. Finalized Deployment and Back-out Plan.
d. Finalized CONOPS
e. Finalized CMaaS Solution documentation.
f. Finalized Plan for Transition to Production Operations.
g. Finalized Security Model and Accreditation Package.
h. Plan for Production Operations.

The specific deliverables are:

1. Documents noted above
2. Presentation materials
3. Demonstration of solution
4. Baseline schedule (IMS) and TBOM
5. Identification of Next Steps
    a. Plan for resolution of UAT/ORR outstanding items
    b. Identification of items needs to Transition to O&M
    c. Timeline for Transition to O&M

C.4.4 OPERATIONS AND MAINTENANCE PHASE

After some period of operational maturity, the Operational Test Authority (OTA) may request determination of the operational status of the solution, referenced as the OTRR. This is the appropriate time for a PIR.

For the OTRR/PIR, the Government will review the contractor's CMaaS Solution in production for successful implementation and subsequently determine if expected benefits have been realized, including review of operational data measuring the CMaaS Solution's effectiveness and confirming that it is delivering the desired service and support level. The Government will conduct PIRs periodically throughout the O&M phase and evaluate ongoing operation of the contractor's CMaaS Solution.

The PIR documentation shall distinguish between Shared Services and CMaaS. The RACI roles for security controls must be clear for Shared Services.

The prerequisites to complete the PIR are:

a. Performance Reports.
b. Operational Analysis (**Section F, Deliverable 30**).
c. Ongoing Security Assessments (to include Plans of Action and Milestones (POA&M) tracking).
d. As-built documentation.
e. Finalized Plan for Production Operations.

The specific deliverables are:

1. Documents noted above
2. Presentation materials
3. Demonstration of solution
4. Baseline schedule (IMS) and TBOM

C.5 OBJECTIVE

The objective of the TO is to design, configure and operate a secure Shared Service backbone that supports the CMaaS Solution for the enumerated Agencies that complies with applicable standards and demonstrates improved detection and analysis of IT security events in cooperation with DHS CDM Program Office and the Agencies (as the CDM end users in this TO).

The delivered CMaaS solution shall embody the CDM Structure shown in Figure 8 and meet the operational and functional requirements as detailed in **Section J, Attachments N and N-2 – CMaaS Phase 1 and Phase 2 Requirements** for the in-scope CDM Functional Areas (HWAM, SWAM, CM, VUL, TRUST, BEHAVE, CRED, and PRIV) (identified above in Section C.2, Scope).

C.6 TASKS

C.6.1 TASK 1 – PROVIDE PROJECT MANAGEMENT SUPPORT

The contractor shall provide project management support under this TO beginning at **Project Start (Section F, Deliverable 01)**. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this SOW. The contractor shall identify a Project Manager (PM) by name, who shall serve as the primary interface and point of contact (POC) with the Government on the TO. The PM shall provide management, direction, administration, quality assurance (QA), and leadership of the execution of this TO.

The contractor shall use industry-best standards and proven methodologies that ensure all TO activities are identified, documented, and tracked so that the TO can continuously be evaluated and monitored for timely and quality service. The contractor shall notify the FEDSIM CO and COR of any technical, financial, personnel, Organizational Conflict of Interest (OCI), or general managerial problems encountered throughout the life of the TO.

The contractor shall support privacy compliance activities as needed (H.1.4, H.3.3.3) (**Section F, Deliverable 48).** The contractor shall support DHS to ensure DHS can complete any required Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), or System of Records Notice (SORN) documents or other supporting documentation to support privacy compliance. The contractor shall work with personnel from the DHS CDM Program Office, the NPPD Office of Privacy Office, the DHS Office of the Chief Information Officer (OCIO), the Records Management Branch, and any respective agency Privacy POCs to ensure that the privacy documentation are kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the NPPD Office of Privacy and other offices are answered in a timely fashion.

The contractor shall clearly articulate the technical approach to shared services within the overall CMaaS solution. The Work Breakdown Structure (WBS) shall separate Shared services build out from the rest of the CMaaS Solution.

C.6.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule and coordinate a **Project Kick-Off Meeting (Section F, Deliverable 02)** at the location approved by the Government. The meeting shall provide an introduction between the contractor personnel and Government personnel involved with the TO. The meeting shall also provide the opportunity to discuss technical, management, or security issues, travel authorization, and reporting procedures. At a minimum, the attendees shall include key contractor personnel, representatives from DHS including the TPOC, the CO, the FEDSIM COR, and Government representatives from each Agency supported by this TO. The contractor shall provide a **Kick-Off Agenda and Kick-Off Meeting Presentation (Section F, Deliverable 03)** that shall provide, at a minimum, the following type of information:

a. Introduction of team members and personnel:
   1. Roles and Responsibilities. Include staffing plan and project organization.
   2. Overview of the contractor organization to support multiple Agencies.

b. Communication Plan/Lines of communication overview (between both the contractor and Government).

c. TO Management:

1. Overview/outline of the PMP.
2. Overview of project tasks.
3. Overview of the Integrated Master Schedule (IMS) (shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
4. Identified risks and issues and applicable mitigation plans.
5. Overview of Transition Plan to Operations.
6. Overview of the TEMP.
7. Coordination of SELC Reviews.
8. TO QCP **(Section F, Deliverable 04)** update.
9. TO logistics.

d. TO Administration:
    1. Review of Government-Furnished Information and Equipment (GFI/GFE).
    2. Invoice review and submission procedures.
    3. Travel notification and processes.
    4. Security requirements/issues/facility/network access procedures.
    5. Sensitivity and protection of information.
    6. Reporting requirements, e.g., Monthly Status Report (MSR).
    7. Proposed reports of technical metrics on operation of CMaaS Solution as defined in the PMP.
    8. Additional administrative items.

e. Review of initial deliverables.

The contractor shall draft and provide a **Kick-Off Meeting Minutes Report (Section F, Deliverable 16)** in accordance with Section C.6.1.7, Prepare Meeting Reports**,** documenting the Kick-Off Meeting discussion and capturing any action items.

C.6.1.2 SUBTASK 1.2 – PREPARE A PROJECT MANAGEMENT PLAN (PMP) AND INTEGRATED MASTER SCHEDULE (IMS)

Based on the contractor's proposal in response to the solicitation, the contractor shall prepare and deliver a **Draft and Final PMP (Section F, Deliverables 06 and 07).**

The PMP shall contain at a minimum the following:

a. Management approach:
    1. Communications and stakeholder management
    2. Scope management. Include milestones, tasks, and subtasks required in this TO
        i. Cost management
        ii. Requirements management
    3. Quality management
    4. Staffing management
    5. Procurement management
    6. Logistics management

b. Technical approach:

    1. Work Breakdown Structure (WBS) and WBS dictionary. Include associated responsibilities and partnerships between Government organizations. The WBS should plan for control accounts that allow for tasks to be planned, budgeted, forecasted and cost collected at a level which allows for summary level organized by Agencies. WBS shall separate any Shared Services build out from the other tasks.
    2. Risk management, including identified risks and issues
    3. Testing

c. Training approach

d. Proposed reports of technical metrics on operation of CMaaS Solution, at a minimum to include that it collects data on at least 95 percent of devices in each set of two successive scans within the 72-hour window in accordance with **(Section J, Attachments N and N-2 – CMaaS Phase 1 and Phase 2 Requirements**.

The contractor shall prepare and deliver a **Draft and Final Integrated Master Schedule (Section F, Deliverables 09 and 10)** to accompany the PMP, but as a separate deliverable.

C.6.1.3 SUBTASK 1.3 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP) AND INTEGRATED MASTER SCHEDULE (IMS)

The PMP is an evolutionary document that shall be updated with significant changes as required **(Section F, Deliverable 08).** The contractor shall work from the latest Government-approved version of the PMP.

The IMS is also an evolutionary document that shall be updated with technical inputs and significant changes as required **(Section F, Deliverable 11).** The contractor shall reflect the Government's requirements in planning for all activities in Tasks 2 through 11 and the tailored DHS SELC process reviews in the IMS. This includes the Government's requirements that the CMaaS Solution for each Agency shall be operational as soon as the contractor is able to complete installation, configuration, and required security authorization at individual Agencies. The contractor shall work from the latest Government-approved version of the IMS.

Significant changes represent any alteration, modification, or adjustment to the CMaaS Solution, cost, or schedule that is sufficiently great or important and worthy of attention in the PMP or IMS.

C.6.1.4 SUBTASK 1.4 – PROVIDE MONTHLY STATUS REPORT AND BRIEFING

The contractor shall develop and provide a **Monthly Status Report (MSR) (Section F, Deliverable 12**). The MSR shall briefly summarize, by task area, the TO management and technical progress to date, as well as provide the current information indicated below. The purpose of this report is to ensure all stakeholders are informed of key elements of the CDM project at the Agency level, provide opportunities to allow stakeholder input, and coordinate resolution of risks and issues and change management as required. The contractor shall provide, at a minimum, the following information:

a. Activities during reporting period, by task and subtask, to include: ongoing activities, new activities, activities completed, deliverables submitted for that period, and progress to date on all above mentioned activities. Start each section with a brief description of the task.

b. Up-to-date project schedule showing major tasks, milestones (to include upcoming milestones) and deliverables; planned and actual start and completion dates for each. Assessment of progress (baseline versus actual as depicted in the project schedule), 30-day look ahead for tasks to be completed as shown in the project schedule.

c. Financial status including:
   1. Actual TO burn through the current month, and projected cost of each CLIN broken down by control account as identified in the WBS.
   2. Up-to-date spend plan by control account including baseline, actuals, and forecast.
   3. Chart reflecting funding and burn rate for the month and cumulative.
   4. Cumulative invoiced amounts for each CLIN and labor tasks totals to-date.
   5. Actual current and cumulative dollars expensed for small businesses.

d. Problems and corrective actions taken. Include issues or concerns that may affect project milestones, personnel, and cost resources and proposed resolutions to address them to include risk mitigation plans.

e. Contractor personnel gains, losses, and staffing status of Key and non-Key Personnel (e.g., upcoming leave).

f. Government actions required (e.g., deliverables awaiting Government approval).

g. Summary of trips taken, conferences attended.

h. Summary of logistics tracking (including product purchase, delivery, and installation).

i. Status of action items and status of risks and issues (assessment of mitigation or resolution plans).

j. Recommendations for project change management actions, modifications, or improvements in task or process.

k. Reports of technical metrics on operation of CMaaS Solution as defined in the PMP.

l. Tier II and III Ticket Tracking (see Section C.6.7.1, Provide Tier Two and Tier Three Support to the CMaaS Solution).

The MSR shall be prepared in accordance with the sample provided in **Section J, Attachment B - Monthly Status Report Template**.

The contractor shall also provide a **Monthly Contract Activity and Status Briefing (Section F, Deliverable 13)** with the FEDSIM COR, DHS TPOC, and other key Government stakeholders that provides the status of activities during the reporting period, by task area, to include on-going activities, new activities, activities completed, and progress to date on all items identified above for the MSR. The contractor PM shall provide a meeting report in accordance with Section C.6.1.7, Prepare Meeting Reports, to the FEDSIM COR. The briefing shall be conducted as a teleconference and scheduled every month with the FEDSIM COR, DHS TPOC, and other Government resources to review and discuss the status of the TO and activities. The Government reserves the right to change this requirement to in-person monthly status meetings as required.

C.6.1.5 SUBTASK 1.5 – PROBLEM NOTIFICATION REPORTS (PNRs)

The contractor shall provide a **Problem Notification Report (PNR) (Section F, Deliverable 14)** that notifies the FEDSIM CO and FEDSIM COR of any issues such as potential cost/schedule overruns/impacts and significant technical issues one day after the problem is identified. The PNR shall be prepared in accordance with the sample in **Section J, Attachment I - Problem Notification Report Template.**

C.6.1.6 SUBTASK 1.6 – PREPARE TRIP REPORTS

The contractor shall submit a **Trip Report (Section F, Deliverable 15)**, as requested by the DHS TPOC and/or FEDSIM COR. The contractor shall submit Trip Reports three working days after completion of a trip for all long-distance travel**.**

The Trip Report shall include the following information:

a. Personnel traveled
b. Dates of travel
c. Destination(s)
d. Purpose of trip
e. Summarized cost of the trip
f. Approval authority
g. Summary of events, action items, and deliverables

C.6.1.7 SUBTASK 1.7 – PREPARE MEETING REPORTS

The contractor shall submit **Meeting Reports (Section F, Deliverable 16)** to document results of meetings no later than two workdays following the meeting. The Meeting Report shall include the following information:

a. Meeting attendees and their contact information – at minimum identify organizations represented

b. Meeting dates
c. Meeting location
d. Meeting agenda
e. Purpose of meeting
f. Summary of events (issues discussed, decisions made, and action items assigned)

C.6.1.8 SUBTASK 1.8 – CONVENE IN-PROGRESS REVIEW (IPR)

The contractor shall conduct a formal **In-Progress Review (IPR) (Section F, Deliverable 17)** to be held quarterly at the Government's location. IPRs shall include the FEDSIM COR, DHS TPOC, other key Government stakeholders, and additional Government and contractor representatives deemed necessary by the FEDSIM COR and/or the DHS TPOC. The IPR shall provide a forum for Government review of progress, planning, and issues related to the TO. The contractor shall utilize the PMP in its discussion of TO performance. The contractor shall document and email a **Meeting Report (Section F, Deliverable 16)** in accordance with Section C.6.1.7, Prepare Meeting Reports**,** to IPR participants within two business days. IPRs shall include: schedule by task, previous months activities by task, planned activities for next month by task, and issues/actions required by the Government. The quarterly IPR shall replace the Monthly Status Briefing for that month.

C.6.1.9 SUBTASK 1.9 – FACILITATE TASK ORDER TRANSITION-OUT

The contractor shall facilitate the accomplishment of a seamless transition from itself to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a **TO Transition-Out Plan (Section F, Deliverable 18)** no later than (NLT) 120 calendar days prior to end of the Base Period and updated prior to the end of each Option Period. The TO Transition-Out Plan shall be broken down by Agency. The contractor shall identify how to coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of Contact (POCs)
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a seamless transition
f. Transition of Key Personnel
g. Identify schedules and milestones
h. Identify actions required of the Government
i. Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition
j. Technical details for transferring the CMaaS Solution from the shared services platform to the replacement platform, including data transfer, shared system platform design with diagrams, virtual machines, transfer of operations, and test of the transfer plan.

The Transition Plan shall address the contingency where the Shared Services are provided on the same platform after the transition, but the CMaaS solution transfers to another vendor.

C.6.1.10 SUBTASK 1.10 – IMPLEMENT TASK ORDER TRANSITION-OUT

The contractor shall implement the TO Transition-Out Plan NLT 90 calendar days prior to expiration of the TO. The contractor shall transition the Shared Services in advance of the total CMaaS transition. Shared Services shall be in operation before the other components of the solution.

C.6.1.11 SUBTASK 1.11 – COORDINATE AND COMPLETE SELC REVIEWS

The contractor shall coordinate and complete each SELC review as detailed in Section C.4, DHS SELC Process, for each Agency's CMaaS Solution. Depending on the contractor's implementation schedule, these SELC reviews shall be completed concurrently or separately by Agency.

C.6.2 TASK 2 – CMaaS SOLUTION TECHNICAL PLANNING

The contractor shall provide its proposed approach to implementing the specific in-scope CDM Phase 1 and Phase 2 capabilities in its CMaaS Solution. The CMaaS Solution Technical Planning task shall integrate the contractor's CDM methods and best practices into a sufficiently detailed technical plan, as described in the below Task 2 Subtasks, to ensure successful implementation and operation of the CMaaS Solution at the Agencies supported by this TO.

C.6.2.1 SUBTASK 2.1 – VALIDATE PROPOSED CMaaS SOLUTION

The validation of the proposed CMaaS Solution consists of two parts:

a. The contractor shall perform an "as is" analysis to validate its proposed CMaaS CDM Shared Service Solution against each Agency's existing infrastructure to facilitate better CDM Program and IT architecture planning. The contractor shall report via the PNR (Section C.6.1.5, **Problem Notification Reports - Section F, Deliverable 14**) all discrepancies between information provided by Agencies at pre-solicitation information and their existing environments. The contractor shall be responsible for coordinating the "as-is" analysis with the respective Agencies.

   This analysis shall specifically include analysis of each participating Agency's De-Militarized Zone (DMZ) environments. This analysis shall describe the presence of a firewall and available port density to terminate secure network connections from the Shared Service environment to the Agencies included in this TO. The intent is that the contractor shall provide as part of their solution any augmentation required to support the implementation of the CDM solution.

b. The contractor shall prepare an **Overview of the CMaaS Solution (Section F, Deliverable 20)** for inclusion in the SDR SELC review. The Overview of the contractor's

CMaaS Solution shall include any updates as a result of the “as-is-analysis.”

C.6.2.2 SUBTASK 2.2 – DEVELOP SHARED SERVICES CONCEPT OF OPERATIONS (CONOPS)

The contractor shall develop a **Concept of Operations (CONOPS) (Section F, Deliverable 21)** that describes how the proposed CMaaS Solution architecture shall meet the CDM requirements for the supported Agencies in their respective environments.

The CONOPS shall include, at a minimum, the following:

a. How the CMaaS Solution installs tools and sensors on the covered network and provides an integration point for passing data to the DHS level CDM Dashboard and the Federal Dashboard provided to the contractor. The CONOPS shall contain the specifics for the underlying architecture of both Shared Services and CDM solution infrastructure.

b. Methodology for incorporating data into useful information to support operational, tactical, and strategic decisions for Agencies.

c. Methodology for integrating data from the CMaaS Solution to support decision systems for supported Agencies, including managing technical refresh and upgrades of multiple products.

d. Incorporate CDM-specified security configuration settings, as they become available, to the appropriate toolset.

e. How the CMaaS Solution provides desired and actual state and the resulting difference or defect information of each Agency endpoint necessary to assist the Agency in defect remediation.

C.6.2.3 SUBTASK 2.3 – PREPARE CMaaS SOLUTION IMPLEMENTATION ARCHITECTURE

The contractor shall prepare and deliver a **CMaaS Solution Implementation Architecture and Back-out Plan (Section F, Deliverable 22)** that shall include, at a minimum, the following:

a. Overview graphical representation of the overall CMaaS Solution.
b. Technical architecture and specifications. As appropriate, distinguish between the technical architecture of the Shared Services infrastructure and the CMaaS solution.
c. Data architecture and specifications. As appropriate, distinguish between the data architecture of the Shared Services infrastructure and the CMaaS solution.
d. Interface architecture and specifications. As appropriate, distinguish between the interface architecture of the Shared Services infrastructure and the CMaaS solution.
e. Solution functionality.
f. High level functional requirements.
g. Operational requirements.

h. Plan for reversing implementation if necessary

The CMaaS Solution Implementation Architecture shall elaborate the CMaaS Solution previously described in the Technical Proposal.

The Architecture shall show the entire solution (including the ABCD layers in Figure 8) and shall highlight the Shared Services area. The Architecture shall show connectivity between and across ABCD.

The contractor shall update the CMaaS Solution Implementation Architecture as appropriate to reflect As-Built documentation as part of PIR and deliver the **CMaaS Solution Implementation Architecture – As-Built Update** (**Section F, Deliverable 23**)

C.6.3 TASK 3 – SUPPORT CDM DASHBOARDS

The Government plans to deliver the Agencies' CDM Dashboard(s) to the contractor in support of its CMaaS Solution for each Agency in the Base Year of this TO. The Government plans to provide iterative releases of the Agency's CDM Dashboard between the Initial Operating Capability (IOC) and Final Operating Capability (FOC). The Government's CDM Dashboard Provider will provide the Agency CDM Dashboard initial and on-going support to the contractor for each release of its Agency CDM Dashboard product. The CDM Dashboard Provider will train the contractor in Agency CDM Dashboard installation, integration, and support. The CDM Dashboard Provider will maintain and improve the functional processes within Agency CDM Dashboard software in accordance with the CDM Dashboard TO.

The contractor shall install, configure, and maintain each release of the Government-provided Agency CDM Dashboard for use by the Agencies. The contractor shall provide quality assurance and technical testing for each release of the delivered Agency CDM Dashboard with respect to its interoperation with the CMaaS Solution. The contractor shall ensure that each release of the Agency CDM Dashboard interfaces with the Federal CDM Dashboard.

C.6.3.1 SUBTASK 3.1 – PROVIDE CDM DASHBOARD TECHNICAL SERVICES

Once the Government and CDM Dashboard Provider deliver the Agency CDM Dashboard, and training is delivered to the contractor, the contractor shall install, configure, and transition the Agency CDM Dashboard to production operations.

Additionally, the contractor shall integrate the Agency CDM Dashboard with the Federal CDM Dashboard. The contractor shall ensure that only summary level data is being sent from the Agency CDM Dashboard to the Federal CDM Dashboard. The contractor shall conform to Figure 8, which identifies that the Agency CDM Dashboard shall have data input from a single integrated source. The contractor shall provide an integration point data source for the Agency CDM Dashboard. The contractor shall provide Agency CDM Dashboard testing support consistent with Section C.6.11, Conduct Testing, Support Independent Verification and Validation and System Authorization.

C.6.3.2 SUBTASK 3.2 – PROVIDE AGENCY CDM DASHBOARD TIER TWO SUPPORT

The contractor shall provide Tier Two support to the Agency CDM Dashboard user community including, but not limited to, the following:

a. In-depth troubleshooting.
b. Specialized knowledge of the CMaaS Solution and Agency CDM Dashboards for remediation.
c. Elevation of all calls determined to be related to the Agency CDM Dashboard solution and not resolved through Agency CDM Dashboard Tier Two support and forwarding of these calls to the CDM Dashboard Provider for Tier Three support.

The Agencies will provide the CDM Dashboard Tier One support. Agency CDM Dashboard Tier One support shall include problem resolution using standard methodologies and basic troubleshooting techniques.

The contractor shall provide Agency CDM Dashboard Tier Two support while performing other support consistent with Section C.6.7, Operate CMaaS Solution.

C.6.4 TASK 4 – PROVISION SPECIFIED CMAAS SOLUTION

The contractor shall provide the CMaaS Solution meeting the requirements as described in this TO (see **Section F**, the CMaaS Solution includes IT services **Deliverables 40 – COTS CDM Tools, 41 – Data Provided with CDM Tools (if any), and 44 – Ancillary ODCs/Tool**s).

The contractor shall prepare and update as necessary a **Resource Requirements document (Section F, Deliverable 24)**. At a minimum, this document shall consist of the following:

a. Bill of Materials (BOM) for the CDM Phase 1 and Phase 2 Products (CDM Tools) and the ancillary IT hardware and software (Ancillary ODCs/Tools) **(Section F, Deliverable 25).**
b. GFE, GFI, or Government-Furnished Services (GFS) on which the contractor is relying to develop the CMaaS Solution and meet the TO requirements.
c. Supply Chain Safeguards (see Section H.3.4).
d. Electronic and Information Technology (EIT) Products and Services List (see Section H.5).

The document shall identify items procured for the Shared Services platform as such.

The contractor shall procure and deliver CDM tools and sensors, as identified in the BOM, to support the operation of its CMaaS Solution and in accordance with Section H.8, below. This includes the procurement of any proprietary or public data required for the configuration or operation of the CDM tools and sensors (e.g., a whitelist table of acceptable software, including a complete copy of the table or ongoing access to online tables). The contractor shall identify, procure, and install ancillary IT hardware and software as needed, in accordance with Section H.8, Tool (Hardware/Software) And/Or ODCs and H.8.2 ODC Authorization Request. Deliverable terms and conditions are located in Section F, Deliverables or Performance; Delivery and Acceptance is addressed in **Section J, Attachment Q - Delivery and Acceptance Process**.

The Government will execute a TO modification when appropriate for new or changed items in the BOM for tools, sensors, and ancillary hardware and software (e.g., at completion of Validation Subtask 2.1). The contractor shall revise the BOM, as appropriate, for use with the **Product Delivery Data List (PDDL) (Section F, Deliverable 26)** during Delivery and Acceptance (see embedded PDDL template as part of **Section J, Attachment Q - Delivery and Acceptance Process**).

The contractor shall work collaboratively with DHS CDM Program Office and Agencies to manage property accountability, to include the transfer of licenses.

Note: CDM Tools & Ancillary ODCs/Tools

a. *CDM Tools* are those tools to be acquired under the CDM CMaaS BPA (and appearing in the Catalog of Tools Available on Any CDM CMaaS BPA (**Section J, Attachment V))** that are identified in the TBOM and included in the original Technical Proposal. CDM Tools identified in the original Technical Proposal but with increased or decreased quantities identified during Validation Subtask 2.1 are also *CDM Tools*. *CDM Tools* also include additional Cybersecurity tools identified during Validation Subtask 2.1 and not appearing in the original Technical Proposal, but listed in the Catalog of Tools Available on Any CDM CMaaS BPA (**Section J, Attachment V**).

b. *Ancillary ODCs/Tools* includes general-purpose (i.e., not Cybersecurity-specific) hardware and software that are not available on the CDM CMaaS BPA but are required in order to provide a complete solution. All Ancillary ODCs/Tools, except non-IT items, must be available and acquired under an existing GSA Schedule contract. Ancillary ODCs may also include items other than information technology. Priced Government-off-the-Shelf (GOTS) software tools, if any are proposed, are also Ancillary ODCs/Tools.

C.6.5 TASK 5 – CONFIGURE AND CUSTOMIZE CMAAS SOLUTION

The contractor shall install, configure, and customize its CMaaS Solution to accomplish the objectives of this TO. The CMaaS Solution shall include the actual state, desired state, and any deviations between the desired state and the actual state for each capability.

Configuration also includes configuration of the Shared Services that provide the platform for the CDM Solution. Configuration of the Shared Services shall include compliance with the CDM Shared Services security controls called out in **Section J, Attachment Y**; isolation of each Agency's solution from the others; connectivity between the Solution and Agency endpoints and intermediate Agency components and networks as required and consistent with the contractor's Technical Approach, Concept of Operations, and Solution Architecture; support of Agency CDM Dashboards and connectivity with the Federal Dashboard; and provides the other Shared Services features called out in Section C.1.

Based on the requirements of each Agency, the contractor shall install, configure, and/or customize the tools, sensors, and any ancillary equipment identified in its CMaaS Solution consistent with **Section J, Attachment G - Agency IT/Network Environment Summary Information,** additional information disclosed during Section C.6.2, CMaaS Solution Technical Planning, and with the IMS and the PMP.

The contractor shall design the CMaaS Solution for minimal network performance impact as a result of implementing its CMaaS Solution. **Section J, Attachments N and N-2 – CMaaS Phase 1 and Phase 2 Requirements** define minimal impact as, "Limit the burden put on network resources such that the presence of the scan is not noticeable above background variation in network bandwidth."

It is permissible to include free open source software, free proprietary software, free or priced GOTS software, or other non-COTS software in the CMaaS Solution (except that only CDM CMaaS BPA software may be used for cybersecurity functions (HWAM, SWAM, etc.)), but such software is subject to the Government's technical evaluation (see, e.g., Section M.6.1).

The Government anticipates that no new software development (as opposed to configuration of COTS tools) will be required under this TO. However, in the event that new software development is required, the following applies, as does Section H.11, New Software.

C.6.5.1 SUBTASK 5.1 - SOURCE, OBJECT, EXECUTABLE AND RUN-TIME CODE

The contractor shall provide the most current version(s) and release(s) of any and all source, object, executable, and run-time code (as applicable) developed under the efforts of this TO ("New Code") and unique enhancements, customization, and plug-ins, and other similar artifacts ("Customizations") to the Government **(Section F, Deliverable 45)** in accordance with the delivery requirements in Section F.8, New Software Delivery. The parties agree that payments made under this TO constitute full payment for any data rights in New Code. The Government's requirements for data rights in the New Code and Customizations are specified in Section F.8, New Software, and FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007). The contractor shall ensure that all COTS licenses and Open Source licenses both allow for the creation of the Customizations and vest the data rights to the Customizations exclusively in the Government.

DHS CDM Program Office will have unlimited rights to use and modify all source, object, executable, and run-time code (as applicable) comprising the New Code, and its associated documentation, even in the event that the contractor shall become unable to continue supporting the CMaaS Solution, and the contractor, immediately upon delivery (each deliverable accompanied by a signed assignment of copyright), shall assign copyright in such New Code to the Government as contemplated under the FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007). Source, object, executable, and run-time code (as applicable), including scripts and enhancements, comprising the New Code for releases of the software produced under this TO shall become the property of the Government upon such assignment. The source, object, executable, and run-time code (as applicable), with its associated documentation and other materials as specified in Section F.8, New Software Delivery, shall be delivered to DHS CDM Program Office on dates established in accordance with Section F, Deliverables or Performance, but in any event, no later than 30 calendar days following the termination/expiration of the TO.

In the event the contractor defaults on the terms of this TO for any reason, the most current version of the source, object, executable, and run-time code shall be delivered to DHS CDM Program Office no later than 30 calendar days following the event that leads to the termination/expiration of the TO; the Government will retain the right to use any and all versions that are at that time installed at a Government facility, and to further develop and distribute them, with no further royalties or other payments being due to the contractor or any other party.

C.6.6 TASK 6 – MAINTAIN DATA ON DESIRED STATE FOR CMAAS SOLUTION

A key component of the CMaaS Solution is the desired state specification, maintained in a data form that can be easily compared to the actual state of Agency assets. The Agencies will establish the criteria for desired state.

The contractor shall work with each Agency and incorporate the desired state information authorized by each Agency into its CMaaS Solution, to include automation necessary to improve and maintain timeliness of information. The detailed specifications for HWAM, SWAM, CM, VUL, TRUST, BEHAVE, CRED, and PRIV desired state covered by this task are defined in **Section J, Attachments N and N-2 – Phase 1 and Phase 2 Requirements**.

The following table identifies a non-inclusive list of desired state specifications examples:

Type of Desired State Specification	Examples:
Desired state	If software product X is present, setting Z should have value Y to increase security
Prohibited state	If software product X is present, the following patch levels have CVEs that produce risk, and are prohibited. List of product patch levels, with associated CVEs and composite risk for each.
Expected state	If software product X is present, the device should have a list of executables with hashes to identify them. It may be partially installed.

Table 3: Examples of Desired State Specifications

C.6.7 TASK 7 – OPERATE CMAAS SOLUTION

The operational requirements in this task apply to the CDM Shared Service Solution, to include the Agency CDM Dashboard and associated data feeds, as identified in Areas A, B, and C of Figure 8.

The contractor shall conduct the operation of the CDM Shared Service Solution, including the installed suite of CDM tools and sensors. This support may be provided either on-site at the Agency's location(s), from the CDM Shared Service facility, from an alternate location, or in combination. While Agency-designated system administrators will have access to the CDM tools and sensors, including their product consoles, the contractor shall be responsible for the operation of the overall CMaaS Solution.

The contractor shall operate the CMaaS Solution in conformance with the SLOs (C.6.7.5 and **Section J, Attachment C**).

C.6.7.1 SUBTASK 7.1 – PROVIDE TIER TWO AND TIER THREE SUPPORT TO THE CMaaS SOLUTION

The contractor shall coordinate its Tier Two and Tier Three support with the Agencies' and CDM Dashboard Provider's Help Desks. The contractor shall provide Tier Two and Tier Three support for the CMaaS Solution, except Tier Three support for the CDM Dashboard, which will be provided by the CDM Dashboard Provider.

The contractor shall provide hot-line capability during the normal workweek (Monday through Friday) and shall provide coverage from 0800 through 1800 hours Eastern Time (ET).

a. The Agencies will provide Tier One support. Tier One support will include problem resolution using standard methodologies and basic troubleshooting techniques including Agency-raised issues, incident and request management, access and inventory management, change and configuration management, security, and patch management consistent with Agency's policies and procedures.

b. The contractor shall provide Tier Two support. Tier Two support shall include more in-depth troubleshooting and shall require specialized knowledge of CMaaS Solution and Agency CDM Dashboards for remediation.

c. The contractor shall provide Tier Three support for the CMaaS Solution. Tier Three support shall include advanced engineering support to include coordination and resolution with Solution original equipment manufacturers (OEMs). All calls determined by Tier Two to be related to the CDM Dashboard and not resolved through Tier Two shall be forwarded to the CDM Dashboard Provider for Tier Three support.

The contractor shall establish a procedure for recording and a ticket tracking mechanism for all operational support requests. The contractor shall report on a monthly basis the ticket inflow to include the total number of tickets received, types of issues, and how they were resolved in the MSR (see Section C.6.1.4, Provide Monthly Status Report). The contractor shall, at a minimum, provide the following support:

a. Provide initial problem resolution where possible.
b. Generate, monitor, and track incidents through resolution.
c. Provide software support.
d. Maintain **Frequently Asked Questions (FAQs) (Section F, Deliverable 27)** and their resolutions.
e. Obtain customer feedback and conduct surveys.

C.6.7.2 SUBTASK 7.2 – PREPARE A PLAN FOR PRODUCTION OPERATIONS

The contractor shall develop a **Plan for Production Operations (see Section F, Deliverable 28)**. The Plan for Production Operations shall describe how the contractor shall operate the proposed CMaaS Solution architecture to meet CDM objectives outlined in this TO after DHS CDM Program Office acceptance of the CMaaS Solution at completion of the ORR/OTRR. The Plan for Production Operations shall include, at a minimum, the following:

a. Testing Methodology (in support of Section C.6.11, Conduct Testing, Support Independent Verification and Validation and System Authorization) to include the TEMP (see Section C.6.11.1, Conduct Testing on CMaaS Solution).

b. Implementation Methodology:

   1. Provide considerations for risk mitigation such as:
      i. Demonstration of CMaaS Solution implementation.
      ii. Initial pilot to test the CDM infrastructure with defined success criteria.
      iii. Phased implementation approach.
      iv. User Acceptance Test.
      v. Submission of software as part of baseline configuration image.
   2. Roll out of functionality consistent with IMS.
   3. **Documentation of Agency Dependencies (Section F, Deliverable 29)**.
   4. Description of configuration management methodology for the tools and sensors of the CMaaS Solution. Plan shall include incorporation of CDM services on all assets of the Agency's infrastructure, including applications, servers, and desktops.
   5. Distribution of CDM tools and sensors to ensure that the CMaaS Solution collects data on at least 95 percent of devices in each set of two successive scans within the 72-hour window in accordance with **Section J, Attachments N and N-2 - Phase 1 and Phase 2 Requirements**.

c. O&M Methodology

   1. Identify requirements needed to operate the CMaaS Solution through the entire life of the TO.
   2. Describe detailed activities that support the CMaaS CONOPS.
   3. Determine data relevant for inclusion in MSR.
   4. Describe Operational Analysis (**Section F, Deliverable 30**) for PIRs.
   5. Description of configuration management methodology for the tools and sensors of the CMaaS Solution.
   6. Description of Change Management methodology for the tools and sensors of the CMaaS Solution.

C.6.7.3 SUBTASK 7.3 – PERFORM PRODUCTION OPERATIONS

The contractor shall operate the CMaaS Solution consistent with the Plan for Production Operations. The contractor shall monitor the CMaaS Solution for system performance and functionality and elevate any issues. The contractor shall incorporate the CMaaS Solution into the respective Agencies' continuous monitoring activities. The CMaaS Solution shall operate consistent with the system security requirements as identified in Section C.6.11, Conduct Testing, Support Independent Verification and Validation (IV&V) and System Authorization.

The contractor shall perform problem management in coordination with the Agencies for the CMaaS Solution by identifying problems and performing resolution, to include notifying OEM vendors of application issues. The contractor shall initiate formal requests for any Agency infrastructure modifications and follow change control procedures. The contractor shall provide technical support for all CDM Solution components and the solution as a whole, whether from a single source or multiple sources (see H.9.4).

The contractor shall submit reports of technical metrics on the operation of CMaaS Solution as defined in the approved PMP in the MSR.

C.6.7.4 SUBTASK 7.4 – PERFORM SYSTEM ADMINISTRATION

The contractor shall perform system administration to operate the CMaaS Solution throughout the TO period of performance. The contractor shall, at a minimum, provide the following support pending Agency change management approval:

a. Patching
b. Upgrades
c. Replacement of failed components of the CMaaS Solution

The contractor shall identify patching and upgrades of the Shared Services platform separately from the other components and levels of the CMaaS Solution.

C.6.8 TASK 8 – INTEGRATE AND MAINTAIN INTEROPERABILITY BETWEEN CMAAS SOLUTION AND AGENCY LEGACY APPLICATIONS AND DATA

The contractor shall integrate and maintain interoperability between the CMaaS Solution and other Agency legacy applications for the purpose of sharing data. **Section J, Attachments N and N-2 – Phase 1 and Phase 2 Requirements** provide details on the interoperability requirements.

C.6.8.1 SUBTASK 8.1 – INTEGRATE INTEROPERABILITY BETWEEN CMaaS SOLUTION AND AGENCY LEGACY APPLICATIONS

The contractor shall integrate legacy applications that provide authoritative information for CDM Phase 1 and Phase 2, within the scope of this TO, specific to IT asset information and policy definitions, into the CMaaS Solution. The contractor shall establish the data exchange mechanism between the CMaaS Solution and Agency legacy applications that hold the authoritative information. This activity is in support of Section C.6.6, Maintain Data on Desired State for CMaaS Solution. Examples of legacy applications include, but are not limited to, the following:

a. Discovery tools.
b. Network asset systems (e.g., Active Directory and other Lightweight Directory Access Protocol (LDAP)-like systems).
c. Property management systems.
d. Configuration management systems.
e. Vulnerability management systems.
f. Open Checklist Interactive Language (OCIL) questionnaire systems.

C.6.8.2 SUBTASK 8.2 – MAINTAIN INTEROPERABILITY BETWEEN CMAAS SOLUTION AND AGENCY LEGACY APPLICATIONS

The contractor shall periodically perform the appropriate data exchanges between the Agency legacy applications and the CMaaS Solution as outlined in **Section J, Attachments N and N-2 – Phase 1 and Phase 2 Requirements** to ensure the CMaaS Solution uses the most current data as defined by the Agency policy. The contractor shall update the data exchange mechanism in response to changes in either the Agency legacy applications or the CMaaS Solution.

C.6.9 TASK 9 – OPERATE DATA FEEDS TO/FROM INSTALLED CDM DASHBOARDS

The contractor shall establish the data exchange mechanisms, utilizing the Security Content Automation Protocol (SCAP)-compliant Asset Summary Reporting Format (ASR), between the following:

a. The CMaaS Solution integration point and Agency CDM Dashboard(s) (Area B and Area C of Figure 8).
b. All Agency CDM Dashboard(s) (within Area C of Figure 8).
c. The Agency CDM Dashboard(s) to the CDM Federal Dashboard - summary level data only (between Area C and Area D of Figure 8).

The contractor shall operate and maintain the CDM Dashboard data feeds (as identified in this task) consistent with Section C.6.7, Operate CMaaS Solution.

C.6.10 TASK 10 – PROVIDE GOVERNANCE SUPPORT AND CMaaS SOLUTION TRAINING

Each Agency is responsible for managing its implementation of CDM and the associated policies. The contractor shall use CDM governance guidelines that are being developed by the DHS CDM Program Office to provide governance support to the Agencies. In addition, the contractor shall provide CMaaS Solution training, per the subtasks below.

C.6.10.1 SUBTASK 10.1 – PROVIDE CDM GOVERNANCE SUPPORT

The DHS CDM Program Office will provide CDM Program Governance guidance to the contractor. The contractor shall use its knowledge of its CMaaS Solution, its CDM Program expertise, and the DHS CDM Program Office-provided CDM Program guidance to assist the

Agencies to develop or improve Agency-specific CDM governance structures and policies.

The contractor shall deliver a **Draft and Final CDM Governance Support Plan (Section F, Deliverables 31 and 32)** for each of the supported Agencies. The CDM Governance Support Plan shall include:

a. Assessment of existing cybersecurity governance environment (including processes, organizational structures, and relationships) at the Agency.

b. Recommendations/best practices to establish, modify or improve, and manage each Agency's CDM Program, following DHS guidance. Recommendations/best practices shall include at a minimum the following:

    1. Processes for developing or improving and managing Agency-specific CDM governance structures.
    2. Integration of DHS CDM governance best practices into Agency ISCM/CDM or broader information security governance structures and policies.
    3. Process for developing and/or updating the Agency's ISCM strategy required by OMB Memorandum M-14-03.
    4. Strategy for establishing/improving and managing Agency-specific Information Security Continuous Monitoring (ISCM)/CDM working groups and encouraging Agency participation in the DHS CDM working groups.
    5. The contractor shall provide a recommendation outlining the structure and level of effort of the ongoing support of CDM governance (primarily consisting of CDM working group(s).

The contractor shall conduct initial working group(s) for presenting CDM governance to the Agency CDM stakeholders.

C.6.10.2 SUBTASK 10.2 – PROVIDE CMaaS SOLUTION TRAINING

The contractor shall provide training on implementation and operations of the specific CMaaS Solution in the Agencies' environments. Contractor training shall include providing core **CMaaS Solution Training Documentation (see Section F, Deliverable 33)** consisting of all training materials, any training manuals, and COTS manuals for all CDM products. This training shall adhere to the approach detailed in the contractor's Government-approved PMP. The training approach shall, at a minimum, include the following:

a. Training Method
b. Training Medium
c. Training Tools
d. Frequency of Training
e. Audience
f. Location
g. Method to incorporate training feedback

The contractor shall ensure all training is consistent with the DHS-provided CDM program training content. The DHS CDM training content provides an overview of CDM concepts, principles, and approaches for all phases of the CDM Program and how CDM capabilities work together. DHS CDM training, including Phase 1 and Phase 2 capabilities, is currently offered through in-person sessions to the Agencies and through self-study/online formats to contractors. Information on the self-study materials can be accessed through the GSA BPA Holder Google Portal (accessible to the contractor after TO2F TO award). Information will be provided electronically through other formats when available.

At the minimum, the contractor shall deliver the following CMaaS Solution-based training:

a. A CMaaS Solution overview and orientation training shall be conducted prior to deployment of the CMaaS Solution at each Agency as identified in the PMP.
b. CMaaS Solution technical training shall be conducted at the time of the installation of the CDM tools and sensors. This shall consist of detailed CMaaS Solution product configuration, integration, and operation training as it relates to an Agency's network environment. This training is not intended to replace manufacturer's certification training.
c. CDM Dashboard technical training shall be conducted at the time that the CDM Dashboard is integrated into the CMaaS Solution at the Agency.

The CDM Dashboard Provider will provide standardized FOC CDM Dashboard training materials to the contractor when delivering the CDM Dashboard. The contractor shall present content specific to its CMaaS Solution as it relates to the standardized CDM Dashboard training content with consideration of Agency unique environments.

The contractor's CMaaS Solution Training Documentation shall be provided to the DHS TPOC and FEDSIM COR for review/approval prior to delivery to the Agencies.

C.6.11 TASK 11 – CONDUCT TESTING, SUPPORT IV&V AND SYSTEM AUTHORIZATION

The contractor shall provide the project management, engineering, data, and documentation necessary to conduct testing, support IV&V efforts, and support system authorization as required by the TO.

C.6.11.1 SUBTASK 11.1 – CONDUCT TESTING ON CMaaS SOLUTION

The contractor shall deliver a draft and final **TEMP (Section F, Deliverables 34 and 35)** that ensures delivery of a quality CMaaS Solution to the Agencies supported within this TO. The TEMP is expected to be a living document and is anticipated to be updated periodically throughout the PoP of this TO **(Section F, Deliverable 36)**. The TEMP must be inclusive of all testing activities including, at a minimum:

a. Testing approach:

    1. Critical test parameters.
    2. Evaluation criteria.
    3. Developmental test and evaluation method.
    4. Operational test and evaluation methods for verifying technical and functional requirements.
    5. Automated test tools.
    6. Resource management.
    7. A CMaaS Solution specific Requirements Traceability Matrix (RTM).

b. Testing methodologies:

    1. Identify the testing tool sets.

2. Description of the intended test environment.

c. Milestone schedules.

d. Test cases and associated test plans.

e. Test results reports.

The contractor shall follow the approved TEMP throughout the TO performance to produce test plans, conduct the testing, and generate reports. The contractor shall provide all test plans to the DHS TPOC for review and approval prior to performing the formal testing.

The contractor shall establish a testing capability/process. The testing capability/process shall provide support ensuring all integrated applications are compatible and interoperable with all deployed Agency CMaaS Solution components prior to installation within the Agency production environment. The contractor shall provide testing support for initial installation and subsequent updates of its CMaaS Solution which shall be coordinated with the DHS TPOC (and respective Agency representatives) for system acceptance. All test results and problems shall be logged, tracked, and available upon the Government's request. The contractor shall report all major issues that affect the schedule in the PNR (see Section C.6.1.5, **Problem Notification Reports - Section F, Deliverable 14**).

The contractor shall provide integration testing for the Agency-level CDM Dashboard(s) and the respective CMaaS Solution. The CDM Dashboard integration testing shall be incorporated in the TEMP and, at a minimum, shall include the following:

a. Interface testing.
b. Integration testing.
c. Preparation of test plans and procedures.
d. Test reports.
e. Acceptance testing.

The contractor shall perform end-to-end system testing of the CMaaS Solution including testing in a contractor test facility and the Agency designated environments which could include development and testing (dev/test), staging, pre-production, and production. System testing shall include, but not be limited to, the following:

a. Final acceptance testing of the CMaaS Solution including CDM Dashboard.
b. Scalability (network performance).
c. Conducting integration testing of hardware, software, and network.

End-to-end systems testing shall be repeatable to accommodate changes in either the CMaaS Solution or the Agency environment.

The contractor shall support Post-Implementation Reviews (PIR) to include the following:

a. Operational testing in the Agency environment.

b. Evaluating effectiveness of incorporating the CMaaS Solution into the Agencies' CDM governance program.

C.6.11.2 SUBTASK 11.2 – PROVIDE INDEPENDENT VERIFICATION AND VALIDATION (IV&V) SUPPORT

The contractor shall allow DHS CDM PO and/or its designated representatives (e.g., OTA, IV&V Team) to observe and/or participate in all developmental and/or operational tests and evaluations conducted by the contractor.

The Government may conduct additional operational and security-related assessments of the CDM Shared Service Solution. The contractor shall assist with these assessments as directed by the FEDSIM COR or DHS TPOC.

C.6.11.3 SUBTASK 11.3 – PROVIDE SYSTEMS AUTHORIZATION SUPPORT

In accordance with FISMA, the CDM Shared Service Solution at each Agency is required to receive/maintain system security authorization following NIST SP 800-37 Rev. 1 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*.

All CDM Shared Service Solutions have been categorized for FIPS 199 as High Confidentiality, High Integrity, and High Availability. Authorization support includes authorization of the Shared Services.

The contractor shall provide a **Security Model with Documentation (Section F, Deliverable 37)** to update the Accreditation/Authorization Package, as identified below.

The contractor shall perform security authorization activities on the Agencies' CMaaS Solution to include the following:

a. Provide the Agencies with all required documentation to support the Agencies' security authorization (in ongoing authorization format).

b. Provide technical support to the Agencies' security authorization process related to the CDM Shared Service Solution:

    1. Security Test and Evaluation/Security Assessment activities.
    2. Remediation of findings or creation of POA&Ms as appropriate.

c. Incorporation of CMaaS Agency Solution into the Agencies' continuous monitoring activities.